

# **APPENDIX**

**MAKING WARRANTS GREAT AGAIN: AVOIDING GENERAL SEARCHES IN THE  
EXECUTION OF WARRANTS FOR ELECTRONIC DATA**

*Jennifer S. Granick*

**CONTENTS OF THE APPENDIX**

Brief of the ACLU et al. as Amici Curiae Supporting Defendant-Appellant, <i>State v. Hughes</i> , 958 N.W.2d 98 (2020).....	APPENDIX 1
<i>State v. Hughes</i> , 958 N.W.2d 98 (2020).....	APPENDIX 35
Brief of the ACLU et al. as Amici Curiae Supporting Defendant-Appellee, <i>People v. McCavitt</i> , ___ N.E.3d. ___, 2021 WL 4898748 (Ill. 2021).....	APPENDIX 81
<i>People v. McCavitt</i> , ___ N.E.3d. ___, 2021 WL 4898748 (Ill. 2021).....	APPENDIX 125
Brief of the ACLU et al. as Amici Curiae Supporting Defendant-Appellant, <i>State v. Burch</i> , 961 N.W.2d 314 (Wisc. 2021).....	APPENDIX 166
<i>State v. Burch</i> , 961 N.W.2d 314 (Wisc. 2021).....	APPENDIX 199
Brief of the ACLU et al. as Amici Curiae in Support of Motion to Quash Search Warrant, <i>In re Search Warrant to Google for All Records Associated with Google Account Scottarcla@gmail.com</i> , No. 20CCPC0020 (Cal. Super Ct. Aug. 31, 2020).....	APPENDIX 272
<i>In re Search Warrant to Google for All Records Associated with Google Account Scottarcla@gmail.com</i> , No. 20CCPC0020 (Cal. Super Ct. Aug. 31, 2020).....	APPENDIX 302
Brief of the ACLU et al. as Amici Curiae in Support of Appellant, <i>United States v. Cobb</i> , 970 F.3d 319 (4th Cir. 2020).....	APPENDIX 317
<i>United States v. Cobb</i> , 970 F.3d 319 (4th Cir. 2020).....	APPENDIX 354
Brief of the ACLU et al. as Amici Curiae in Support of Defendant-Appellant, <i>United States v. Ganas</i> , 824 F.3d 199 (2d. Cir. 2016).....	APPENDIX 396
<i>Ganas I</i> , 755 F.3d 125 (2d. Cir. 2014).....	APPENDIX 430
<i>Ganas II</i> , 824 F.3d 199 (2d. Cir. 2016).....	APPENDIX 467
Brief of the ACLU of Massachusetts et al. as Amici Curiae in Support of Appellee, <i>Commonwealth v. Snow</i> , 160 N.E.3d 277 (Mass. 2021).....	APPENDIX 528
<i>Commonwealth v. Snow</i> , 160 N.E.3d 277 (Mass. 2021).....	APPENDIX 568
Brief of the ACLU as Amici Curiae in Support of Defendant-Appellant, <i>United States v. Morton</i> , 984 F.3d 421 (5th Cir. 2021).....	APPENDIX 592
<i>United States v. Morton</i> , 984 F.3d 421 (5th Cir. 2021).....	APPENDIX 631
Brief of the ACLU as Amici Curiae in Support of Defendant-Appellant, <i>United States v. Basey</i> , No.18-30121 (9th Cir. mandate issued Oct. 1, 2019)....	APPENDIX 646
<i>United States v. Basey</i> , No.18-30121 (9th Cir. mandate issued Oct. 1, 2019).....	APPENDIX 685

**STATE OF MICHIGAN  
IN THE SUPREME COURT**

On Appeal from the Court of Appeals  
(Jonathan Tukel, P.J., Douglas B. Shapiro and Jane M. Beckering, JJ.)

---

PEOPLE OF THE STATE OF MICHIGAN,

Plaintiff-Appellee,

Supreme Court Case No. 158652

v

Court of Appeals Case No. 338030

KRISTOPHER ALLEN HUGHES,

Lower Court Case No. 2016-260154-FC

Defendant-Appellant.

---

**AMICUS CURIAE BRIEF OF THE CRIMINAL DEFENSE ATTORNEYS OF  
MICHIGAN, THE AMERICAN CIVIL LIBERTIES UNION, AND THE AMERICAN  
CIVIL LIBERTIES UNION OF MICHIGAN IN SUPPORT OF DEFENDANT-  
APPELLANT**

Stuart G Friedman (P46039)  
Friedman Legal Solutions, PLLC  
26777 Central Park Blvd, #300  
Southfield MI 48076  
(248) 228-3322  
[stu@crimapp.com](mailto:stu@crimapp.com)

Attorney for CDAM

Daniel S. Korobkin (P72842)  
American Civil Liberties Union  
Fund of Michigan  
2966 Woodward Ave.  
Detroit, MI 48201  
(313) 578-6824  
[dkorobkin@aclumich.org](mailto:dkorobkin@aclumich.org)

Brett Max Kaufman  
American Civil Liberties Union Foundation  
125 Broad Street, 18th Floor  
New York, NY 10004

Jennifer S. Granick  
American Civil Liberties Union Foundation  
39 Drumm Street  
San Francisco, CA 94114

Attorneys for ACLU and ACLU of Michigan

RECEIVED by MSC 7/31/2020 8:51:12 PM

TABLE OF CONTENTS

TABLE OF AUTHORITIES ..... ii

INTEREST OF *AMICI CURIAE* ..... 1

INTRODUCTION ..... 3

RELEVANT FACTS ..... 5

ARGUMENT ..... 7

I. The Affidavit in Support of the Warrant to Seize and Search Mr. Hughes’s Cell Phone Did Not Establish Probable Cause Because It Offered No Case-Specific Facts Suggesting That Evidence of Drug Trafficking Would Be Found There. .... 7

    A. Affidavits Must Establish Probable Cause That Evidence Will Be Found in the Place To Be Searched. .... 7

    B. An Officer’s “Training and Experience,” Without More, Is Insufficient to Establish Probable Cause to Search. .... 8

    C. Allegations Based Only on “Training and Experience” Are Especially Inadequate When Officers Seek To Seize and Search the Entirety of Someone’s Cell Phone, Which Contains Vast Amounts of Extremely Private and Sensitive Data. .... 11

    D. The Cases Cited by the State Show Only How Training and Experience Can Buttress, Not Substitute For, Other Evidence to Establish Probable Cause to Search a Specific Place. .... 13

II. The Fourth Amendment Prohibited Investigators From Searching for Evidence of a New Crime, At Least Without Seeking a Second Warrant. .... 15

    A. Warrants Must Particularly Identify the Crime For Which Evidence Is Sought and Limit Searches Accordingly. .... 16

    B. The Fourth Amendment Requires That Searches of Electronic Data Be Limited to the Scope of the Warrant. .... 19

    C. The Court of Appeals Wrongly Held That the Initial Warrant Gave the Police Broad License to Search For Evidence of Any Crime at All. .... 23

III. Trial Counsel Was Ineffective for Failing to Challenge the Search of the Cell Phone Data in the Instant Case on Fourth Amendment Grounds. .... 25

CONCLUSION ..... 26

## TABLE OF AUTHORITIES

### Cases

<i>ACLU v Clapper</i> , 785 F3d 787 (CA 2, 2015).....	1
<i>Alasaad v Nielsen</i> , 419 F Supp 3d 142 (D Mass, 2019).....	1
<i>Andresen v Maryland</i> , 427 US 463; 96 S Ct 2737; 49 L Ed 2d 627 (1976).....	16
<i>Arizona v Gant</i> , 556 US 332; 129 S Ct 1710; 173 L Ed 2d 485 (2009).....	7
<i>Berger v New York</i> , 388 US 41; 87 S Ct 1873; 18 L Ed 2d 1040 (1967).....	17
<i>Boyd v United States</i> , 116 US 616; 6 S Ct 524; 29 L Ed 746 (1886).....	7
<i>Carpenter v United States</i> , 585 US __; 138 S Ct 2206; 201 L Ed 2d 507 (2018).....	1, 7, 13
<i>Commonwealth v White</i> , 475 Mass 583; 59 NE3d 369 (2016).....	8
<i>Florida v Harris</i> , 568 US 237; 133 S Ct 1050; 185 L Ed 2d 61 (2013).....	7
<i>Groh v Ramirez</i> , 540 US 551; 124 S Ct 1284; 157 L Ed 2d 1068 (2004).....	15
<i>Horton v California</i> , 496 US 128; 110 S Ct 2301; 110 L Ed 2d 112 (1990); .....	17, 18
<i>Illinois v Gates</i> , 462 US 213; 103 S Ct 2317; 76 L Ed 2d 527 (1983).....	8
<i>Johnson v VanderKooi</i> , __ Mich App __; __ NW2d __ (2019) (Docket Nos. 330536, 330537).....	2
<i>Katz v United States</i> , 389 US 347; 88 S Ct 507; 19 L Ed 2d 576 (1967).....	18
<i>Marron v United States</i> , 275 US 192; 48 S Ct 74; 72 L Ed 231 (1927).....	16

<i>Maryland v Garrison</i> , 480 US 79; 107 S Ct 1013; 94 L Ed 2d 72 (1987).....	16
<i>People v Armstrong</i> , 490 Mich 281; 806 NW2d 676 (2011).....	25
<i>People v Darwich</i> , 226 Mich App 635; 575 NW2d 44 (1997).....	11
<i>People v Frederick</i> , 500 Mich 228; 895 NW2d 541 (2017).....	1
<i>People v Hughes</i> , unpublished per curiam opinion of the Court of Appeals, issued September 25, 2018 (Docket No. 338030) .....	18, 23
<i>People v Hughes</i> , 505 Mich 855; 934 NW2d 273 (2019).....	3
<i>People v Hughes</i> , 943 NW2d 646 (2020) .....	3
<i>People v Nunez</i> , 242 Mich App 610; 619 NW2d 550 (2000).....	10
<i>People v Randolph</i> , 502 Mich 1; 917 NW2d 249 (2018).....	26
<i>People v Russo</i> , 439 Mich 584; 487 NW2d 698 (1992).....	14
<i>People v Whitfield</i> , 461 Mich 441; 607 NW2d 61 (2000).....	13, 14
<i>People v Woodard</i> , 321 Mich App 377; 909 NW2d 299 (2017).....	24
<i>People v Zuccarini</i> , 172 Mich App 11; 431 NW2d 446 (1988).....	11
<i>Riley v California</i> , 573 US 373;134 S Ct 2473; 189 L Ed 2d 430 (2014).....	1, 11, 12, 22
<i>Stanford v Texas</i> , 379 US 476; 85 S Ct 506; 14 L Ed 2d 431 (1965).....	7, 13, 17
<i>State v Thein</i> , 138 Wash 2d 133; 977 P2d 582 (1999) .....	8

<i>Texas v Brown</i> , 460 US 730; 103 S Ct 1535; 75 L Ed 2d 502 (1983).....	8
<i>United States v Brown</i> , 828 F3d 375 (CA 6, 2016).....	8, 10
<i>United States v Carey</i> , 172 F3d 1268 (CA 10, 1999).....	21
<i>United States v Castro</i> , 881 F3d 961 (CA 6, 2018).....	17
<i>United States v Comprehensive Drug Testing, Inc</i> , 621 F3d 1162 (CA 9, 2010) (en banc).....	20, 22
<i>United States v Danhauer</i> , 229 F3d 1002 (CA 10, 2000).....	9
<i>United States v Ellison</i> , 632 F3d 347 (CA 6, 2011).....	8
<i>United States v Frazier</i> , 423 F3d 526 (CA 6, 2005).....	9
<i>United States v Ganas</i> , 824 F3d 199 (CA 2, 2016) (en banc).....	1
<i>United States v Griffith</i> , 432 US App DC 234; 867 F3d 1265 (2017).....	10, 13
<i>United States v Grimmett</i> , 439 F3d 1263 (CA 10, 2006).....	20
<i>United States v Hanna</i> , 661 F3d 271 (CA 6, 2011).....	16
<i>United States v Higgins</i> , 557 F3d 381 (CA 6, 2009).....	9
<i>United States v Hill</i> , 459 F3d 966 (CA 9, 2006).....	7, 21
<i>United States v Jacobsen</i> , 466 US 109; 104 S Ct 1652; 80 L Ed 2d 85 (1984).....	18, 23
<i>United States v Johnson</i> , 848 F3d 872 (CA 8, 2017).....	14

<i>United States v Jones</i> , 159 F3d 969 (CA 6, 1998) .....	9
<i>United States v Jones</i> , 565 US 400; 132 S Ct 945; 181 L Ed 2d 911 (2012).....	1
<i>United States v Katzin</i> , 769 F3d 163 (CA 3, 2014) .....	1
<i>United States v Khounsavanh</i> , 113 F3d 279 (CA 1, 1997).....	9
<i>United States v Lalor</i> , 996 F2d 1578 (CA 4, 1993).....	9
<i>United States v Loera</i> , 923 F3d 907 (CA 10, 2019), certiorari denied 140 S Ct 417 (2019) .....	21
<i>United States v Lyles</i> , 910 F3d 787 (CA 4, 2018).....	9, 10
<i>United States v Otero</i> , 563 F3d 1127 (CA 10, 2009) .....	20, 21
<i>United States v Pitts</i> , 6 F3d 1366 (CA 9, 1993).....	9
<i>United States v Portalla</i> , 496 F3d 23 (CA 1, 2007).....	12
<i>United States v Richards</i> , 659 F3d 527 (CA 6, 2011) .....	20
<i>United States v Rios</i> , 881 F Supp 772 (D Conn, 1995).....	9
<i>United States v Roman</i> , 942 F3d 43 (CA 1, 2019).....	9
<i>United States v Rosario</i> , 918 F Supp 524 (D RI, 1996) .....	9
<i>United States v Ross</i> , 456 US 798; 102 S Ct 2157; 72 L Ed 2d 572 (1982).....	17
<i>United States v Rowland</i> , 145 F3d 1194 (CA 10, 1998).....	9

*United States v Schultz*,  
14 F3d 1093 (CA 6, 1994) ..... 8, 9

*United States v Terry*,  
911 F2d 272 (CA 9, 1990) ..... 9

*United States v Walser*,  
275 F3d 981 (CA 10, 2001), ..... 21, 22

*United States v Wey*,  
256 F Supp 3d 355 (SDNY, 2017) ..... 20

*United States v Williams*,  
974 F2d 480 (CA 4, 1992) ..... 9

*Warden, Md Penitentiary v Hayden*,  
387 US 294; 87 S Ct 1642; 18 L Ed 2d 782 (1967)..... 8

*Wiggins v Smith*,  
539 US 510; 123 S Ct 2527; 156 L Ed 2d 471 (2003)..... 25

**Constitutions and Statutes**

US Const, Am IV ..... 7

Const 1963, art 1, § 11 ..... 7

**Other Authorities**

*CDAM Bylaws*, art 1, sec 2 ..... 2

Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions On Nonresponsive Data*, 48 Texas Law Rev 1 (2015)..... 23

Kerr, *Searches and Seizures in a Digital World*, 119 Harv L Rev 531, 542 (2005) ..... 22

US Dep’t of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009)..... 20

**INTEREST OF *AMICI CURIAE***<sup>1</sup>

The American Civil Liberties Union (ACLU) is a nationwide, nonprofit, nonpartisan organization. The ACLU of Michigan is a state affiliate of the ACLU. Both organizations are dedicated to defending the principles embodied in the Constitution and our nation’s civil rights laws and, for decades, have been at the forefront of efforts nationwide to protect the full array of civil rights and liberties, including the right to the protections enshrined in the Fourth Amendment. The ACLU and the ACLU of Michigan have frequently appeared before courts (including this one) throughout the country in Fourth Amendment cases, both as direct counsel and as amici curiae. *See Carpenter v United States*, 585 US \_\_; 138 S Ct 2206; 201 L Ed 2d 507 (2018) (warrantless acquisition of cellphone location information); *ACLU v Clapper*, 785 F3d 787 (CA 2, 2015) (bulk collection of call records), *United States v Katzin*, 769 F3d 163 (CA 3, 2014) (warrantless GPS tracking), *Alasaad v Nielsen*, 419 F Supp 3d 142, 147 (D Mass, 2019) (warrantless searches of electronic devices at the border), *Riley v California*, 573 US 373; 134 S Ct 2473; 189 L Ed 2d 430 (2014) (cellphone searches incident to arrest), *United States v Jones*, 565 US 400; 132 S Ct 945; 181 L Ed 2d 911 (2012) (warrantless GPS tracking), *United States v Ganius*, 824 F3d 199 (CA 2, 2016) (en banc) (storing hard-drive data not responsive to a warrant for years); *People v Frederick*, 500 Mich 228; 895 NW2d 541 (2017) (warrantless “knock and

---

<sup>1</sup> Pursuant to MCR 7.312(H)(4), amici state that no counsel for a party authored this brief in whole or in part, nor did any such counsel or a party make a monetary contribution intended to fund the preparation or submission of this brief. No person other than amici, their members, or their counsel made such a monetary contribution.

talk”); *Johnson v VanderKooi*, \_\_ Mich App \_\_; \_\_ NW2d \_\_ (2019) (Docket Nos. 330536, 330537) (warrantless fingerprinting).

Since its founding in 1976, Criminal Defense Attorneys of Michigan (“CDAM”) has been the statewide association of criminal defense lawyers in Michigan, representing the interests of the criminal defense bar in a wide array of matters. CDAM has more than 400 members. As reflected in its bylaws, CDAM exists to “promote expertise in the area of criminal law, constitutional law and procedure and to improve trial, administrative and appellate advocacy,” “provide superior training for persons engaged in criminal defense,” “educate the bench, bar and public of the need for quality and integrity in defense services and representation,” and “guard against erosion of the rights and privileges guaranteed by the United States and Michigan Constitutions and laws.” *CDAM Bylaws*, art 1, sec 2. Toward these ends, CDAM regularly conducts training seminars for criminal defense attorneys, publishes a newsletter with articles relating to criminal law and procedure, and provides information to the state legislature regarding contemplated legislation. CDAM is often invited to file amicus curiae briefs by the Michigan appellate courts.

Based on its extensive experience representing indigent criminal defendants in the Michigan courts, CDAM has substantial institutional expertise regarding the protections guaranteed by the Michigan and United States Constitutions. CDAM has a significant interest in review of the question presented because the Court of Appeals’s decision is contrary to clearly established constitutional protections and threatens to subject indigent criminal defendants to improperly broad and arbitrary exercises of police power.

This Court invited CDAM and other amici to file an amicus brief in this matter. *People v Hughes*, 505 Mich 855; 934 NW2d 273 (2019). The Court gave amici permission to file this brief on or before July 31, 2020. *People v Hughes*, 943 NW2d 646 (2020).

## INTRODUCTION<sup>2</sup>

The Court has asked for amici's contributions on five questions related to the propriety of the police search of Kristopher Allen Hughes's cell phone and the use of the information stored there to convict him of robbery. The cell phone was seized pursuant to a warrant issued in the context of a drug trafficking investigation. However, the police did not provide any case-specific, objective facts tying Mr. Hughes's phone to the alleged wrongful acts. Furthermore, investigators subsequently searched the phone for evidence of the different and separate crime of robbery. No magistrate issued a warrant for that search and there was no showing of probable cause. Amici urge the following conclusions in response to the Court's questions, which are explained fully in the argument that follows:

1. *The affidavit in support of the search warrant issued during the criminal investigation into drug trafficking did not authorize police to obtain all of Mr. Hughes's cell phone data.* Search warrants may issue only if there is probable cause to believe that evidence will be found in the place to be searched. The affidavit filed in support of the warrant provided only that in the officer's "training and experience," drug dealers commonly use their phones in connection with their crimes. (App E 33a). But that is not enough to establish probable cause under the Fourth Amendment. Because there was no case-specific evidence connecting the phone to the illicit activity in which Mr. Hughes was

---

<sup>2</sup> Amici thank Thomas McBrien, a student at the NYU School of Law and ACLU Summer 2020 intern, for his significant contributions to this brief.

allegedly involved, the affidavit was insufficient to justify a search of Mr. Hughes's phone.

2. *Mr. Hughes's reasonable expectation of privacy in his cell phone data was not extinguished when the police seized his cell phone and its data in a prior investigation.*  
To satisfy the Fourth Amendment, the face of the warrant must particularly describe the crime for which there is probable cause and the place or things to be searched. Searches may not exceed these boundaries. These Fourth Amendment requirements ensure that the police will not use a warrant as cover to fish through nonresponsive information for evidence of other crimes, as the officers did here. These clear-cut rules serve to protect the ongoing reasonable expectation of privacy Mr. Hughes retained in his cell phone data, which can be intruded upon only when justified by probable cause.
3. *The search of the cell phone data in the instant robbery case was not within the scope of probable cause underlying the search warrant issued during the concurrent criminal investigation into drug trafficking.* Here, the prosecutor in the robbery case directed the forensic analyst to enter search terms associated with the robbery. The relevant evidence was not obtained as a result of the drug crime investigation. Indeed, there is no indication that the cell phone was ever searched for evidence of drug trafficking.
4. *For the reasons above, officers' search of the cell phone data in the instant case was unconstitutional; and*
5. *Trial counsel was ineffective for failing to file a motion to suppress the results of the forensic examination of Mr. Hughes's cell phone.*

## RELEVANT FACTS

Kristopher Hughes was tried three times before a jury found him guilty of an armed robbery that took place on August 6, 2016. The charges related to allegations that Mr. Hughes—with the help of Lisa Weber—robbed the victim’s home. The issue at trial was whether Mr. Hughes was the robber. Ms. Weber was the primary witness identifying Mr. Hughes, but she had credibility problems such that the first two juries could not confidently rely on her identification. (App N 140a, 373a-379a, 401a-405a).

After the third trial, the jury convicted Mr. Hughes. Newly-introduced evidence obtained by searching Mr. Hughes’s cell phone bolstered Ms. Weber’s testimony and made the difference.

Investigators had obtained Mr. Hughes’s phone pursuant to a search warrant in a separate and unrelated investigation of drug trafficking. Detective Matthew Gorman submitted the affidavit supporting the search warrant, stating that a confidential informant had tipped off the police that Mr. Hughes and an accomplice were selling drugs and in possession of crack cocaine, large amounts of money, and weapons. (App E 39a, ¶ 5). It also stated that, while undercover, the detective purchased drugs from Mr. Hughes’s alleged partner in crime while Mr. Hughes was present. (*Id.* at 40a, ¶ 9). The affidavit in support of the search warrant, however, made no mention of a robbery. The warrant, dated August 11, 2016, authorized police to seize “any . . . devices capable of digital or electronic storage” to search for “any records pertaining to the receipt, possession and sale or distribution of controlled substances.” (App E 30a).

While the affidavit established probable cause that Mr. Hughes was involved in narcotics trafficking, the only allegations in the affidavit suggesting that evidence of that crime would be on Mr. Hughes’s cell phone was an assertion that in the affiant’s training and experience “drug traffickers commonly use electronic equipment to aid them in their drug trafficking activities.”

(App E 38a-42a). Officers executed the warrant the following day and obtained Mr. Hughes's cell phone from his person during a pat down search. (App N 318a).

At Detective Gorman's request, Detective Wagrowski, who has expertise in cell phone forensics, initiated a forensic examination of the phone on August 23, 2016. (*Id.* at 325a). The detective accomplished this using Cellebrite, the brand name for a forensic tool designed to extract all the data from a phone. (*Id.* at 325a-326a). The detective generated a report containing data extracted from the phone. (*Id.* at 327a; App G 48a-51a). This information included text messages, call logs, photographs, and other data. (App N 327a). According to Detective Wagrowski, the report was more than 600 pages long and contained "over 2,000 call logs, [] over 2,900 text message[s] or SMS messages, and over 1,000 pictures." (*Id.* at 329a).

The next step in any forensic process is to conduct a search of the extracted data. Almost all data seizures end up with far more raw data than a person can reasonably review manually, such as the thousands of text messages and photographs on the phone in this case. Thus, digital querying—using keywords or other criteria—is often essential to any device search and seizure because it can effectively winnow the huge amounts of data to that information the searcher is looking for. The record does not reflect, however, that investigators ever searched the report for evidence of drug trafficking.

At some later point—the timing of which is unclear, but perhaps months later—the prosecutor asked Detective Wagrowski to search the 600-plus-page report for evidence of the robbery, specifically communications between Mr. Hughes and Ms. Weber. The detective searched for three phone numbers: two belonging to Ms. Weber and one belonging to the victim. (*Id.* at 329a). The detective also searched the records for words such as "Lisa," "Kris," and various iterations of Mr. Hughes's alleged nickname, "Killer." (*Id.* at 334a-338a). The results of

these searches were introduced in the third robbery trial as Prosecution Exhibits 4-6 and 9-15. (App G 48a-51a; App H 52a-57a; App I 58a-63a). The jury then convicted Mr. Hughes.

## ARGUMENT

### **I. The Affidavit in Support of the Warrant to Seize and Search Mr. Hughes’s Cell Phone Did Not Establish Probable Cause Because It Offered No Case-Specific Facts Suggesting That Evidence of Drug Trafficking Would Be Found There.**

#### **A. Affidavits Must Establish Probable Cause That Evidence Will Be Found in the Place To Be Searched.**

The United States and Michigan Constitutions protect people against unreasonable searches and seizures by requiring that all search warrants be based on probable cause and describe with particularity the places and items to be seized and searched. US Const, Am IV; Const 1963, art 1, § 11. These provisions are meant to protect against general warrants, a hated English practice that allowed a general rummaging through the life of anybody suspected of a crime. See *Stanford v Texas*, 379 US 476, 481; 85 S Ct 506; 14 L Ed 2d 431 (1965) (general warrants were “the worst instrument of arbitrary power . . . that ever was found in an English law book”), quoting *Boyd v United States*, 116 US 616, 624; 6 S Ct 524; 29 L Ed 746 (1886).

The probable cause requirement protects people in two ways: it ensures there is adequate justification for a search, see *Arizona v Gant*, 556 US 332, 345; 129 S Ct 1710; 173 L Ed 2d 485 (2009), and it limits the scope of the search based on the warrant, see *United States v Hill*, 459 F3d 966, 973 (CA 9, 2006). This requirement serves the goal of the Fourth Amendment “to place obstacles in the way of a too permeating police surveillance.” *Carpenter*, 138 S Ct at 2214 (citation and quotation marks omitted).

A police officer has probable cause to conduct a search when “the facts available to [him] would ‘warrant a [person] of reasonable caution in the belief’” that contraband or evidence of a crime is present. *Florida v Harris*, 568 US 237, 243; 133 S Ct 1050; 185 L Ed 2d 61 (2013),

quoting *Texas v Brown*, 460 US 730, 742; 103 S Ct 1535; 75 L Ed 2d 502 (1983) (alterations in original). An affidavit supporting a search warrant must indicate “that contraband or evidence of a crime will be found in a particular place.” *Illinois v Gates*, 462 US 213, 238; 103 S Ct 2317; 76 L Ed 2d 527 (1983). There must “be a nexus . . . between the item to be seized and criminal behavior.” *Warden, Md Penitentiary v Hayden*, 387 US 294, 307; 87 S Ct 1642; 18 L Ed 2d 782 (1967); accord *United States v Brown*, 828 F3d 375, 382 (CA 6, 2016) (requiring that affidavits must set forth “sufficient facts demonstrating why the police officer expects to find evidence in the [place to be searched] rather than in some other place”) (citation omitted). This connection must be specific and concrete, not vague or generalized. See *Brown*, 828 F3d at 375.

**B. An Officer’s “Training and Experience,” Without More, Is Insufficient to Establish Probable Cause to Search.**

An officer’s training and experience alone is not sufficient to establish probable cause. While training and experience may be relevant to determining probable cause, it cannot substitute for specific facts. See *United States v Schultz*, 14 F3d 1093, 1097 (CA 6, 1994); *Commonwealth v White*, 475 Mass 583, 584–585; 59 NE3d 369 (2016); *State v Thein*, 138 Wash 2d 133, 147–148; 977 P2d 582 (1999) (broad generalizations in affidavit that drug dealers often store their drugs at home were insufficient to establish probable cause). This holds even in situations in which decades of experience lead an officer to believe that evidence could be found in a certain place. See, e.g., *Brown*, 828 F3d at 384 (“[I]f the affidavit fails to include facts that directly connect the residence with the suspected drug dealing activity . . . it cannot be inferred that drugs will be found in the defendant’s home—even if the defendant is a known drug dealer.”). A supporting affidavit must allege facts specific to the investigation, such as a reliable confidential informant purchasing drugs in a suspect’s home, to establish probable cause to search that particular place. See *United States v Ellison*, 632 F3d 347, 349 (CA 6, 2011); *United*

*States v Jones*, 159 F3d 969, 974–975 (CA 6, 1998); *cf. United States v Higgins*, 557 F3d 381, 390 (CA 6, 2009); *United States v Frazier*, 423 F3d 526, 532 (CA 6, 2005).<sup>3</sup>

Training and experience may buttress actual, particularized facts, perhaps even establishing probable cause where it would otherwise be absent. But permitting a search based solely on an officer’s experience in other cases and general evidence of wrongdoing in this one “would be to invite general warrants authorizing searches of any property owned, rented, or otherwise used by a criminal suspect—just the type of broad warrant the Fourth Amendment was designed to foreclose.” *United States v Schultz*, 14 F3d 1093, 1097–1098 (CA 6, 1994); accord

---

<sup>3</sup> See also, e.g., *United States v Roman*, 942 F3d 43, 51–52 (CA 1, 2019) (“We have further expressed skepticism that probable cause can be established by the combination of the fact that a defendant sells drugs and general information from police officers that drug dealers tend to store evidence in their homes.” (quotation marks and citation omitted)); *United States v Lyles*, 910 F3d 787, 793–794 (CA 4, 2018) (“The government invites the court to infer from the trash pull evidence that additional drugs probably would have been found in Lyles’s home. Well perhaps, but not probably.”); *United States v Danhauer*, 229 F3d 1002, 1006 (CA 10, 2000) (repetitive statements about the defendants’ house and allegations that the defendants were manufacturing drugs were insufficient to establish probable cause to search the house); *United States v Rowland*, 145 F3d 1194, 1204 (CA 10, 1998) (“Probable cause to search a person’s residence does not arise based solely upon probable cause that the person is guilty of a crime.”); *United States v Khounsavanh*, 113 F3d 279, 285 (CA 1, 1997) (controlled buy was not per se sufficient to establish probable cause to search a residence); *United States v Lalor*, 996 F2d 1578, 1582–1583 (CA 4, 1993) (“residential searches have been upheld only where some information links the criminal activity to the defendant’s residence”), quoting *United States v Williams*, 974 F2d 480, 481–482 (CA 4, 1992); *United States v Rosario*, 918 F Supp 524, 531 (D RI, 1996) (“While this court acknowledges the extensive training and expertise of agent Kelleher, her statements in the affidavit simply provide generalized information regarding how drug traffickers operate.”); *United States v Rios*, 881 F Supp 772, 776–777 (D Conn, 1995) (officer’s general averments based on training and experience do not, standing alone, constitute a substantial basis for the issuance of a search warrant). Some courts have ruled the opposite way. See, e.g., *United States v Pitts*, 6 F3d 1366, 1369 (CA 9, 1993) (“[I]n the case of drug dealers, evidence is likely to be found where the dealers live.”), citing *United States v Terry*, 911 F2d 272, 275 (CA 9, 1990).

*United States v Griffith*, 432 US App DC 234, 244; 867 F3d 1265 (2017); *People v Nunez*, 242 Mich App 610, 622–624; 619 NW2d 550 (2000) (O’CONNELL, J., concurring). Drug dealers often keep controlled substances in their homes, purses, or cars. But police generally are not permitted to search these places without investigation-specific reasons to believe evidence will be found there. See *Brown*, 828 F3d at 385. The same principle applies to cell phones. *United States v Lyles*, 910 F3d 787, 795 (CA 4, 2018) (probable cause to believe that residence was connected to drug trafficking insufficient basis for searching phone found on the premises); *Griffith*, 867 F3d at 238, 243 (allegation that in the affiant’s experience gang members “maintain regular contact with each other” and “often stay advised and share intelligence about their activities through cell phones and other electronic communication devices and the Internet” insufficient to justify search of home for cell phone).

Here, Detective Gorman’s affidavit alleged only that in the officer’s experience, people who are engaged in drug trafficking store records or other relevant information about that crime on digital devices. But training and experience alone do not establish probable cause that evidence of a suspected crime will be found on the cell phone of a particular suspect. The confidential informant whose reports provided the basis for the search warrant reported “observations and conversations” that contributed to probable cause to believe that Mr. Hughes was dealing crack cocaine. (App E 39a-40a). The informant did not report any controlled substance-related electronic conversations or record-keeping involving the cell phone.

Indeed, courts must ensure that investigators do not evade the Fourth Amendment by uttering magic words, including “based on my training and experience.” This is especially true when the thing to be searched or seized, such as a cell phone, is not contraband. See *Griffith*, 867 F3d at 1275 (“Because a cell phone, unlike drugs or other contraband, is not inherently illegal,

there must be reason to believe that a phone may contain evidence of the crime.”). Were an allegation that criminals generally used their cell phones to communicate or take photos sufficient to establish probable cause, police would be able to get a warrant to search digital media in essentially every single drug case—and perhaps even every criminal case—without ever having any specific reason to believe evidence of a crime would be found there. If that were the law, any suspicion of virtually any crime could be the basis for invasive government searches of our most private data.

While the Michigan Court of Appeals has sometimes upheld searches based on generalized “training and experience” affidavits, see *People v Darwich*, 226 Mich App 635, 636–640; 575 NW2d 44 (1997); *People v Zuccarini*, 172 Mich App 11, 15–16; 431 NW2d 446 (1988), those decisions were wrong. This Court should follow the weight of authority and hold that the Fourth Amendment requires case-specific facts in order to establish probable cause to search a cell phone.

**C. Allegations Based Only on “Training and Experience” Are Especially Inadequate When Officers Seek To Seize and Search the Entirety of Someone’s Cell Phone, Which Contains Vast Amounts of Extremely Private and Sensitive Data.**

Case-specific evidence establishing probable cause is especially important when officers aim to search cell phones, which are nearly ubiquitous and contain vast quantities of private information. In *Riley*, 573 US at 394, the United States Supreme Court noted that the top-selling smart phone had a standard capacity of sixteen gigabytes, which “translates to millions of pages of text, thousands of pictures, or hundreds of videos.” Just five years later, the top-selling smart

phones<sup>4</sup> came standard with four times the storage capacity.<sup>5</sup> That storage holds individuals’ family messages, business information, personal photos, location records, browsing history, political conversations, calendars, prescription and health information, and many other extremely sensitive categories of information. See *id.* at 394–396. Additionally, these devices “are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy.” *Id.* at 385. As a result, most Americans now walk around with the entirety of their private lives contained in their pockets. “It would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone.” *Id.* at 399.

The State cites *United States v Portalla*, 496 F3d 23 (CA 1, 2007), to support the idea that cell phones are “essential tools of [the] drug trade,” Pl’s-Appellee’s Supp Br 20 (alteration in brief), and thus worthy of search and seizure even without evidence of their use in criminal acts. But the State’s brackets hide an important word: “their.” In *Portalla*, the court upheld the conviction of a man designated as a drug trafficking co-conspirator because he knowingly sold “throwaway” phones to drug traffickers. *Id.* at 25. No such evidence was presented in the affidavit here.

More fundamentally, cell phones are not “essential tools of the drug trade” like firearms, drug paraphernalia, or triple-beam scales, except to the extent that they are essential tools of

---

<sup>4</sup> See Porter, *Apple and Samsung Dominate Top Selling Phone Lists for 2019*, The Verge (February 28, 2020) <<https://www.theverge.com/2020/2/28/21157386/iphone-best-selling-phone-worldwide-xr-11-samsung-a-series-counterpoint-research>> (accessed July 30, 2020).

<sup>5</sup> See iPhone X  <<https://www.apple.com/shop/buy-iphone/iphone-xr>> (accessed July 30, 2020).

everyday life. None of those objects also serve as their owners' journals, calendars, political organizing tools, etc. As the D.C. Circuit has noted, "[a] warrant's overbreadth [was] particularly notable because police sought to seize otherwise lawful objects: electronic devices. Courts have allowed more latitude in connection with searches for contraband items like 'weapons [or] narcotics.'" *Griffith*, 867 F3d at 1276, quoting *Stanford*, 379 US at 486.

An officer's ability to rummage through the entirety of virtually every person's life based solely on their training and experience is the exact kind of "too permeating police surveillance" that the Fourth Amendment was designed to thwart. *Carpenter*, 138 S Ct at 2214. When the "place" to be searched is something as sensitive as a cell phone, it is not reasonable to accept an officer's conclusory statements about drug traffickers' general habits to serve as the entirety of probable cause. Searches of these devices must be supported by sufficiently specific probable cause lest everyone's most private effects be open to investigation upon mere suspicion of criminal conduct.

**D. The Cases Cited by the State Show Only How Training and Experience Can Buttress, Not Substitute For, Other Evidence to Establish Probable Cause to Search a Specific Place.**

An officer's training and experience can help establish probable cause to search a specific location, but it cannot do so alone. *People v Whitfield*, 461 Mich 441, 442–448; 607 NW2d 61 (2000), cited by the State, does not support the State's argument to the contrary—indeed, it proves amici's point. In *Whitfield*, an undercover officer went to a suspect's house, requested heroin, saw envelopes commonly used to package heroin, and was told he would be "take[n] care [of]" if he came back later with a trusted associate. *Id.* at 447. Objective evidence—the suspicious envelopes and conversation—formed the necessary probable cause, albeit interpreted through the lens of the officer's training and experience. The magistrate properly relied on the

officer's knowledge and experience in concluding that the envelopes, which may have looked innocent to a layperson, were indeed suspicious. See *id.*

Nor can the "nature of the crime" substitute for evidence of probable cause—and the State cites cases in support of that assertion that do not actually help its position. For example, the State cites *United States v Johnson*, 848 F3d 872, 878 (CA 8, 2017), see Pl's-Appellee's Supp Br 17, but there, the affidavit in support of the search warrant incorporated an interview with a child who said the defendant Johnson "downloaded the pictures [of her naked] on his computer that he has at his mom's house in Woodbury," "always downloaded all his pictures on the computers at his mom's house in Woodbury," and "returned to Woodbury 'at least once a week.'" *Id.* at 878 (first alteration in original). It was this factual evidence, not solely the officer's training and experience suggesting that people who commit child sexual abuse crimes store illegal images on computers, that provided the justification for searching Johnson's mother's house. *Id.* Similarly, in *People v Russo*, 439 Mich 584; 487 NW2d 698 (1992), training and experience did not form the entire basis for probable cause, but only served to support the assertion that probable cause was not stale. There, the actual basis of probable cause tying evidence of child sexual assault to Russo's house was an interview with the victim who remembered that assaults had happened in the house, was shown photographic evidence of the assaults in the house afterwards, and knew exactly how the evidence was stored there. *Id.* at 598.

Ultimately, officers must provide some specific reason why they believe evidence of a specific crime will be found in a specific place, and cell phones are no exception. This should not be an onerous requirement for the police, who often use confidential informants to text and call suspected drug dealers. Holding that officers may cite "training and experience" to look through

the entirety of a person's phone would expose people's most private details whenever they rightly or wrongly came under police suspicion.

Here, the affidavit provided insufficient information connecting Mr. Hughes's cell phone with drug trafficking crimes. It may be that drug dealers often use their phones to store evidence of their crimes, but without facts establishing that Mr. Hughes was using *this* phone to store evidence of *his* crimes, there is no probable cause to seize the phone. For these reasons, amici answer this Court's first question in the negative: The affidavit in support of the drug trafficking search warrant was inadequate, the warrant was improper, and the seizure and any subsequent searches of the phone were unconstitutional.

## **II. The Fourth Amendment Prohibited Investigators From Searching for Evidence of a New Crime, At Least Without Seeking a Second Warrant.**

Even if the warrant authorizing the search and seizure of Mr. Hughes's phone in connection with the drug investigation had been appropriate, the officers' subsequent search of the phone for evidence of robbery was not. The Fourth Amendment "requires particularity in the warrant," which is meant to restrict investigators' discretion as to what and where to search. See *Groh v Ramirez*, 540 US 551, 557; 124 S Ct 1284; 157 L Ed 2d 1068 (2004). Warrants must provide a description of the type of evidence sought. *Id.* They may authorize searches only for evidence of the crime for which the affidavit establishes probable cause, and no other. Moreover, officers may conduct searches only as authorized by the warrant.

The particularity requirement is especially important in the context of digital searches in which the entirety of a person's private life is in the hands of the police. It may be reasonable for police to over-seize digital data (for example, an entire hard drive or cell phone) because it is so voluminous and intermingled with non-responsive information that sorting through it at the scene of a seizure is not practicable. But it is unreasonable for the police to capitalize on the logistical

difficulties of digital evidence collection to affirmatively search for evidence of crimes for which there is no probable cause showing and no warrant. Otherwise, each warrant authorizing the search of a cell phone, computer, or online service for evidence of a particular crime would automatically become a general warrant that allowed a rummaging through the entirety of a person's private life. The Fourth Amendment forbids this result.

**A. Warrants Must Particularly Identify the Crime For Which Evidence Is Sought and Limit Searches Accordingly.**

To prevent exploratory rummaging in a person's belongings, the Fourth Amendment's particularity requirement requires that a warrant give investigators sufficient guidance as to where to search and what to search for. *Marron v United States*, 275 US 192, 196; 48 S Ct 74; 72 L Ed 231 (1927). Warrants must prevent invasive "fishing expeditions" by authorizing searches only for evidence of a crime for which there is probable cause. See *Maryland v Garrison*, 480 US 79, 84; 107 S Ct 1013; 94 L Ed 2d 72 (1987) (this "requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit"). The particularity requirement "prevents the seizure of one thing under a warrant describing another." *Andresen v Maryland*, 427 US 463, 479; 96 S Ct 2737; 49 L Ed 2d 627 (1976).

It is not good enough for a warrant to simply identify the places or items to be searched; the warrant must also specifically describe what agents are permitted to search *for*. "[T]he scope of a warrant should be confined to evidence relating to a specific crime, supported by probable cause." *United States v Hanna*, 661 F3d 271, 286 (CA 6, 2011). Warrants authorizing searches for evidence of "crime" must be explicitly or implicitly narrowed to the specific crime for which probable cause has been shown. See *Andresen*, 427 US at 479. Without that narrowing, the

warrant would be unconstitutionally overbroad. See, e.g., *id.*; *United States v Castro*, 881 F3d 961, 965 (CA 6, 2018).

The particularity requirement is even more important when the privacy interests in the place to be searched are highly sensitive. In *Stanford*, 379 US at 511–512, for example, the Supreme Court explained that “the constitutional requirement that warrants must particularly describe the ‘things to be seized’ is to be accorded the most scrupulous exactitude when the ‘things’ are books, and the basis for their seizure is the ideas which they contain.” In *Berger v New York*, 388 US 41, 56; 87 S Ct 1873; 18 L Ed 2d 1040 (1967), the Supreme Court similarly stated that the need for particularity “is especially great in the case of eavesdropping” because such surveillance “involves an intrusion on privacy that is broad in scope.”

The particularity requirement demonstrates, and helps ensure, that individuals retain an expectation of privacy in places and effects for which there is no probable cause to search. The purpose of the particularity requirement is to protect these private places and effects from “rummaging,” as the particularity of the warrant limits the permissible scope of the search. For example, a valid warrant to search for a rifle in someone’s home does not permit officers to open a medicine cabinet where a rifle could not fit. See *Horton v California*, 496 US 128, 141; 110 S Ct 2301; 110 L Ed 2d 112 (1990); *United States v Ross*, 456 US 798, 824; 102 S Ct 2157; 72 L Ed 2d 572 (1982). A person retains a reasonable expectation of privacy in the contents of their medicine cabinet, even if investigators had authority to search for a rifle in the home.

More than that, a warrant to search for one kind of evidence does not extinguish a persons’ expectation of privacy with respect to other, subsequent searches at all. The mere fact that police executed a valid search of a house for evidence of one kind on one day does not permit them to return to search for evidence of other crimes thereafter on the theory that the

original search eliminated the person's expectation of privacy. Searches of personal devices and data are no different in this fundamental respect. Warrants permit officers to invade a legitimate expectation of privacy for a particular purpose—to execute a specific search—consistent with the restrictions on police power set forth in the Fourth Amendment. Those restrictions ensure that any invasion of privacy is reasonable, no more invasive than necessary, and justified under the circumstances. Consequently, a warrant does not extinguish a person's expectation of privacy wholesale, forever, and for all purposes. It permits a carefully limited intrusion. Searches for items that would be evidence of other crimes not described in the warrant are unconstitutional because they are, in effect, warrantless searches—and warrantless searches that do not fall into any exception are by definition unreasonable. See *Katz v United States*, 389 US 347, 357; 88 S Ct 507; 19 L Ed 2d 576 (1967).

In this case, the Court of Appeals held that, because Mr. Hughes's data already had been lawfully extracted from his phone pursuant to the August 12 search warrant, he no longer had any reasonable expectation of privacy in that data. See *People v Hughes*, unpublished per curiam opinion of the Court of Appeals, issued September 25, 2018 (Docket No. 338030), p 3. That is wrong. A seizure deprives an individual of control over their property but does not reduce their reasonable expectation of privacy in the contents of the property. See *Horton*, 496 US at 133. That is why, “[e]ven when government agents may lawfully seize such a package to prevent loss or destruction of suspected contraband, the Fourth Amendment requires that they obtain a warrant before examining the contents of such a package.” *United States v Jacobsen*, 466 US 109, 114; 104 S Ct 1652; 80 L Ed 2d 85 (1984). Warrants require probable cause and particularity exactly because searching for evidence of an unrelated crime is not permitted, even when the object is lawfully seized.

Indeed, the warrant in this case was issued as part of a drug trafficking investigation, and nothing else. Critically, the warrant on its face authorized police to seize “any . . . devices capable of digital or electronic storage” to search for “any records pertaining to the receipt, possession and sale or distribution of *controlled substances*.” (App E 30a). Neither the affidavit nor the warrant refer in any way to a robbery; thus, the warrant did not and could not authorize a search for evidence of that crime. The investigators’ use of keywords to find evidence of that crime under the auspices of a drug dealing investigation is akin to officers looking in the medicine cabinet under the auspices of searching for an illegal firearm. It is a violation of the Fourth Amendment’s warrant requirement and is unconstitutional.

**B. The Fourth Amendment Requires That Searches of Electronic Data Be Limited to the Scope of the Warrant.**

For practical reasons, officers must frequently seize an entire electronic device and make a copy of the information stored there in order to conduct a lawful search of the data at a later point in time. See Fed R Crim P 41(e)(2)(B) (establishing a seize-first, search-second procedure for electronically stored information, where searches are “consistent with the warrant”). This overseizure is reasonable only because it would be even more unreasonable for the police to camp out in a person’s home or business for weeks while segregating responsive from non-responsive data.

But these practical investigatory considerations do not mean that the Fourth Amendment’s particularity provisions cease to apply once the government overseizes digital information. Indeed, the Department of Justice’s own computer search and seizure manual explains the seize-then-search process. Investigators generally must remove storage media for off-site analysis and create an “image copy” of the hard drive—in other words, extracting the data (a seizure) followed by a later search. During the search, the hard drive “is examined and

*data that falls within the scope of the warrant* is identified.” US Dep’t of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 86 (2009) (emphasis added). “[A] computer search may be as extensive as reasonably required *to locate the items described in the warrant*.” *Id.*, citing *United States v Grimmett*, 439 F3d 1263, 1270 (CA 10, 2006) (emphasis added). The guidelines correctly note that “[w]hen an agent searches a computer under the authority of a warrant, however, the warrant will often authorize a search of the computer only for evidence of certain specified crimes.” *Id.* at 90.

Years ago, the Ninth Circuit anticipated the investigators’ actions in the instant case, warning that “[t]he process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect.” *United States v Comprehensive Drug Testing, Inc*, 621 F3d 1162, 1177 (CA 9, 2010) (en banc). If anything, access to digital information makes a carefully particularized search of that data all the more important because officers could readily abuse their access to information outside the scope of their warrant, which they ordinarily would not be permitted to see. *See United States v Richards*, 659 F3d 527, 538 (CA 6, 2011) (“The modern development of the personal computer and its ability to store and intermingle a huge array of one’s personal papers in a single place increases law enforcement’s ability to conduct a wide-ranging search into a person’s private affairs, and accordingly makes the particularity requirement that much more important.”), citing *United States v Otero*, 563 F3d 1127, 1132 (CA 10, 2009).

Because the particularity requirement limits the scope of a search pursuant to a warrant, when police overseize data for one search they cannot later use the same over seized data to conduct a second search outside the scope of the initial warrant. For example, in *United States v Wey*, 256 F Supp 3d 355, 407 (SDNY, 2017), the court likened a warrantless second search of

digital information outside the scope of the first warrant to “the Government seizing some hard-copy notebooks while leaving others it deemed unresponsive behind, and then returning to the premises two years later to seize the left-behind notebooks based on investigative developments but without seeking a new warrant.” See also *United States v Loera*, 923 F3d 907, 922 (CA 10, 2019) (search for child pornography unlawful because it was plainly outside the scope of a warrant to search for computer fraud), certiorari denied 140 S Ct 417 (2019); *Hill*, 459 F3d at 974–975 (“the officer is always limited by the longstanding principle that a duly issued warrant, even one with a thorough affidavit, may not be used to engage in a general, exploratory search”) (quotation marks and citation omitted).

Two influential cases from the Tenth Circuit show that officers may not search for evidence of a separate crime not identified in the warrant in the course of a digital search. In *United States v Carey*, 172 F3d 1268, 1270 (CA 10, 1999), a police officer searched a laptop for evidence of drug distribution pursuant to a warrant. While searching the laptop, the officer stumbled upon child pornography. *Id.* at 1271. At this point, he began searching for and opening files he believed were likely to contain child pornography, instead of continuing to search only for evidence of drug distribution. *Id.* at 1273. The officer’s “unconstitutional general search” violated the suspect’s expectation of privacy in data not described in the warrant, so the evidence was suppressed. *Id.* at 1276.

In *United States v Walser*, 275 F3d 981, 984–985 (CA 10, 2001), the facts were similar to *Carey*, but the investigator, upon unexpectedly finding child abuse images, “immediately ceased his search of the computer hard drive and . . . submit[ted] an affidavit for a new search warrant specifically authorizing a search for evidence of possession of child pornography.” Because the officer did not search for evidence of the new crime of possession of illicit images without

authorization from the magistrate in the form of a warrant based on probable cause, the materials were properly admitted into evidence. *Id.* at 987.

In Mr. Hughes’s case, Detective Wagrowski extracted the information from the phone pursuant to the search warrant issued in the earlier drug case. (App N 326a). There is no indication that officers ever searched the 600-page report for evidence of that crime. But at least a month, and maybe months later, the prosecutor in the armed robbery case asked the forensic officer to search the data for calls and texts between Mr. Hughes’ phone, and those of Ms. Weber and the victim. (App N 329a). Officers did not obtain the evidence of robbery inadvertently. Rather, they intentionally and explicitly searched the phone outside of the parameters of the existing warrant. This subsequent search was unlawful.<sup>6</sup>

---

<sup>6</sup> This is not a case in which the evidence of robbery was in plain view, which is why neither the Court of Appeals nor the State raised the issue below. Plain view, a doctrine that was developed in the context of physical-world searches, requires the government to have been lawfully searching for evidence of the crime identified in the warrant and then stumble upon evidence of a different crime. At that point, the investigators must go get a new warrant. *Walser*, 275 F3d 981, 984–985. Here, the prosecution was searching for evidence of the robbery not identified in the warrant and did not seek a second warrant.

However, this Court should be careful not to suggest that the plain view doctrine could license overbroad searches on different facts. Courts and commentators have repeatedly recognized that, in light of the great volume and variety of information contained in computers, greater protections are required for searches of electronic devices and data than for searches of physical items. See *Riley*, 573 US at 394–395; see also *Comprehensive Drug Testing, Inc.*, 621 F3d at 1175; Kerr, *Searches and Seizures in a Digital World*, 119 Harv L Rev 531 (2005). Courts and scholars have considered several different approaches to this problem. The various opinions in *Comprehensive Drug Testing* propose a menu of potential solutions. See *Comprehensive Drug Testing*, 621 F3d at 1179–1180 (KOZINSKI, C.J., concurring) (“summ[ing] up” the court’s guidance). One option is to require the use of independent review teams to “sort[], segregat[e], decod[e] and otherwise separat[e] seizable data (as defined by the warrant) from all other data,” so as to shield investigators from exposure to information beyond the scope of the warrant. *Id.* at 1179; see *id.* at 1168–1172 (per curiam opinion of the Court). Another is to require the use of technology, including “hashing tools,” to identify responsive files “without actually opening the files themselves.” *Id.* at 1179 (KOZINSKI, C.J., concurring). And yet another is to “waive reliance upon the plain view doctrine in digital evidence cases,” full stop—in other words, to agree not to take advantage of the government’s unwillingness or inability to conduct digital searches in a

**C. The Court of Appeals Wrongly Held That the Initial Warrant Gave the Police Broad License to Search For Evidence of Any Crime at All.**

The cases the Court of Appeals relied on, see *Hughes*, unpub op at 3, do not undermine the longstanding and clear-cut requirement that officers search only for evidence of the crime for which a magistrate found probable cause and which is particularly described in the text of a warrant. The court's reliance on cases in which individuals had lost their expectation of privacy was misplaced, because in this case the warrant to search Mr. Hughes's phone for evidence of a specific crime did not extinguish Mr. Hughes's expectation of privacy in all the data on his phone.

In *United States v Jacobsen*, 466 US 109, 104 S Ct 1652; 80 L Ed 2d 85 (1984), cited by the Court of Appeals, see *Hughes*, unpub op at 3, the officers' warrantless search of a cardboard box containing suspicious white powder was constitutional only because it did not exceed an earlier private search of the box. See *Jacobsen*, 466 US at 120. Moreover, the Court had to ask the question of whether the field test of the powder inside the box was a search requiring a warrant exactly because, if the test were something other than a "yes/no" indicator of the evidence of contraband, it would have invaded the owner's expectation of privacy. See *id.* at 122. *Jacobsen* does not resemble the facts here: Mr. Hughes did not lose a reasonable expectation of privacy in all of his data such that a search outside of the scope of the warrant

---

particularized manner. *Id.* at 1180; see *id.* at 1170–1171 (per curiam opinion of the Court). Additionally, Professor Orin Kerr has argued that the best way to minimize unwarranted intrusions of privacy in electronic searches is to impose use restrictions on nonresponsive data discovered during a lawful search. "[A]gents should only be allowed to use the evidence that is actually described in the warrant. Nonresponsive data found in the course of the search for responsive data should generally be walled off from further use." Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions On Nonresponsive Data*, 48 Texas Law Rev 1, 18 (2015). To avoid unconstitutional general searches, Fourth Amendment law must ensure that investigators are not be able to take advantage of the unique properties of digital storage and reap a windfall by opening non-responsive files and discovering evidence of some other crime.

would be lawful, just because there was a search warrant authorizing investigation for a particular specified crime.

The Court of Appeals also cited *People v Woodard*, 321 Mich App 377; 909 NW2d 299 (2017), a case involving a consensual blood draw, in which the court held that the defendant could not withdraw consent for blood-alcohol analysis after already having consented to a blood draw for that purpose. See *Hughes*, unpub op at 3. *Woodard* is a narrow ruling related only to a consensual blood draw in the context of an intoxicated driving investigation. See *Woodard*, 321 Mich App at 387 (“[W]e conclude that society is not prepared to recognize a reasonable expectation of privacy in the alcohol content of a blood sample voluntarily given by a defendant to the police for the purposes of blood alcohol analysis.”). Mr. Hughes, on the other hand, did not consent to the search of his phone, and the warrant at issue was necessarily limited in scope to evidence of drug distribution. The Court of Appeals implied that there is no meaningful difference between performing blood-alcohol analysis on blood drawn consensually for that purpose, and performing a wide-ranging search for evidence of multiple crimes in cell phone data seized via a warrant based on one specific crime. See *Hughes*, unpub op at 3. On the basis of this inapt analogy, the court would throw out decades of clear constitutional law prohibiting searches for evidence of crimes not named in the warrant. This is error.

If initial overzeal and authorization to search all data extinguished Mr. Hughes’s reasonable expectation of privacy in his data, then every warrant to search for data within an electronic device would effectively authorize the police to search any and all data within the device for evidence of any crime, or even just out of perverse curiosity. Such a holding would thoroughly undermine the legal requirement that a warrant be based on probable cause and particularly describe the things to be searched. The Court of Appeals’ analysis extrapolates from

dissimilar cases a holding that runs headlong into long-established Fourth Amendment jurisprudence.

For these reasons, amici answer the Court's second, third, and fourth questions in the negative. Mr. Hughes's reasonable expectation of privacy in his cell phone data was not extinguished when the police obtained the cell phone data in the prior criminal investigation for drug trafficking. The Fourth Amendment's safeguards are designed to protect that expectation of privacy while authorizing a reasonable invasion—*i.e.*, a particularized search—consistent with a probable-cause finding by a neutral and detached magistrate.

The search of the cell phone data in the instant robbery case was not within the scope of the search warrant issued during the criminal investigation into drug trafficking. The search was conducted after the initial data seizure at the request of the prosecutor in the robbery case for evidence of contacts between Mr. Hughes, his alleged accomplice Ms. Weber, and the robbery victim. Because this was a search for evidence of a crime for which there was no warrant, it is presumptively unconstitutional, and no exceptions to the warrant requirement apply.

### **III. Trial Counsel Was Ineffective for Failing to Challenge the Search of the Cell Phone Data in the Instant Case on Fourth Amendment Grounds.**

Amici agree with Mr. Hughes that his attorney was ineffective. To establish ineffective assistance of counsel, a criminal defendant must show that counsel's performance fell below an objective standard of reasonableness and that and that the deficiency prejudiced the defense. *Wiggins v Smith*, 539 US 510, 521; 123 S Ct 2527; 156 L Ed 2d 471 (2003); *People v Armstrong*, 490 Mich 281, 289–290; 806 NW2d 676 (2011). Apparently, the trial attorney represented Mr. Hughes in the drug case as well as the robbery case. He should have examined the statement of probable cause in the context of that case and learned that there were no factual allegations in

support of the warrant beyond the officer's training and experience. Straightforward legal research would have revealed that that allegation alone is insufficient.

Moreover, the attorney should easily have seen that the subsequent search in the robbery case was unlawful even if the warrant were valid. As the arguments and cases cited above show, well-established Fourth Amendment jurisprudence makes clear that officers could not search Mr. Hughes' cell phone for evidence of any crime except the drug distribution. Every case to have considered the issue has held that searches may only be conducted for evidence of the crime for which there is probable cause.

To establish ineffective assistance of counsel, a defendant must also show that "the deficiencies prejudiced the defendant," meaning there is "a reasonable probability that, but for counsels' unprofessional errors, the result of the proceeding would have been different." *People v Randolph*, 502 Mich 1, 9; 917 NW2d 249 (2018) (quotation marks omitted). Mr. Hughes was tried twice, and the jury twice unable to reach agreement, before prosecutors introduced evidence from the illegal search at trial and finally obtained a conviction. Here, there exists a reasonable probability that, had the trial attorney not failed to assert these clear constitutional arguments, the key evidence convicting Mr. Hughes would have been suppressed.

### CONCLUSION

The judgment of the Court of Appeals should be reversed.

July 31, 2020

/s/ Stuart G. Friedman  
Stuart G. Friedman (P46039)  
Friedman Legal Solutions, PLLC  
26777 Central Park Blvd, #300  
Southfield MI 48076  
(248) 228-3322  
stu@crimapp.com

Attorney for CDAM

Respectfully submitted,

/s/ Daniel S. Korobkin  
Daniel S. Korobkin (P72842)  
AMERICAN CIVIL LIBERTIES UNION  
FUND OF MICHIGAN  
2966 Woodward Ave.  
Detroit, MI 48201  
(313) 578-6824

Brett Max Kaufman  
AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION  
125 Broad Street, 18th Floor  
New York, NY 10004

Jennifer S. Granick  
AMERICAN CIVIL LIBERTIES  
UNION FOUNDATION  
39 Drumm Street  
San Francisco, CA 94114

Attorneys for ACLU and ACLU of Michigan

RECEIVED by MSC 7/31/2020 8:51:12 PM

# Syllabus

Chief Justice:  
Bridget M. McCormack

Chief Justice Pro Tem:  
David F. Viviano

Justices:  
Stephen J. Markman  
Brian K. Zahra  
Richard H. Bernstein  
Elizabeth T. Clement  
Megan K. Cavanagh

**This syllabus constitutes no part of the opinion of the Court but has been prepared by the Reporter of Decisions for the convenience of the reader.**

Reporter of Decisions:  
Kathryn L. Loomis

## PEOPLE v HUGHES

Docket No. 158652. Argued on application for leave to appeal October 7, 2020. Decided December 28, 2020.

Following a jury trial, Kristopher A. Hughes was convicted in the Oakland Circuit Court, Hala Jarbou, J., of armed robbery, MCL 750.529, and was sentenced as a fourth-offense habitual offender, MCL 769.12, to 25 to 60 years in prison. On the evening of August 6, 2016, Ronald Stites was at his home with Lisa Weber, whom he had met earlier that day. Weber had agreed to spend the night with Stites and perform sexual acts in exchange for money. At some point during the evening, Weber called a drug dealer known as “K-1” or “Killer” in order to obtain drugs and asked him to come to Stites’s residence. A man arrived at the residence, sold Stites and Weber crack cocaine, and departed. Later that night, the drug seller returned to Stites’s home with a gun and stole a safe that was located in Stites’s bedroom. Weber later identified defendant as the drug dealer and robber, but Stites was not able to identify the perpetrator. A detective submitted a warrant affidavit to search defendant’s property for evidence related to separate allegations of drug trafficking. The affidavit included information from a criminal informant that defendant and another man were dealing drugs, and the detective asserted that drug traffickers commonly use mobile phones and other electronic equipment in the course of their activities. The district court, Cynthia Thomas Walker, J., concluded that there was sufficient probable cause to support a search warrant and authorized a warrant to search three properties and a vehicle connected with defendant. While executing a search at one of the addresses identified in the warrant, the police detained defendant and seized a cell phone found on his person. Another detective performed a forensic examination of the phone and extracted all of the phone’s data. The extraction software separated the data into categories, including photographs, call logs, and text messages. According to the detective, the software also enabled police to search the data for search terms or specific phone numbers. About a month after the data was extracted, the prosecutor in the armed-robbery case against defendant asked the detective to conduct a second search of defendant’s cell-phone data for contacts with the phone numbers of Stites and Weber; for the names “Lisa,” “Kris,” or “Kristopher”; and for the word “killer.” These searches revealed several calls and text messages between defendant and Weber on the night that Stites was robbed, including text messages from Weber to defendant indicating the location of Stites’s home, that the home was unlocked, and that it had a flat-screen TV. After his conviction, defendant appealed, arguing that the phone records should have been excluded from the trial because the warrant that authorized the search of his phone’s data permitted officers to search for evidence of drug trafficking, not armed robbery. Defendant also argued that trial counsel was ineffective for failing to object to the admission of

the data on Fourth Amendment grounds. The Court of Appeals, TUKEL, P.J., and BECKERING and SHAPIRO, JJ., rejected these arguments and affirmed defendant's conviction in an unpublished per curiam opinion. Defendant sought leave to appeal in the Supreme Court, which ordered oral argument on the application. 505 Mich 855 (2019).

In a unanimous opinion by Justice MARKMAN, the Supreme Court, in lieu of granting leave to appeal, *held*:

1. The Fourth Amendment of the United States Constitution protects against unreasonable searches and seizures. Although a warrant is not always required before a search or seizure, there is a strong preference for searches conducted pursuant to a warrant, and the general rule is that police officers must obtain a warrant for a search to be reasonable under the Fourth Amendment. Under *Riley v California*, 573 US 373 (2014), general Fourth Amendment principles apply with equal force to searches of cell-phone data. In this case, the issue was whether officers violated the Fourth Amendment when they searched defendant's cell phone for *evidence of armed robbery* without obtaining a new warrant when the phone was seized pursuant to a warrant authorizing the search of the phone's data for *evidence of drug trafficking*. The prosecutor argued that defendant lost the reasonable expectation of privacy in his cell-phone data when the phone was seized and the data was searched pursuant to the drug-trafficking warrant. However, under *Riley*, citizens generally maintain a reasonable expectation of privacy in their cell-phone data that is not extinguished merely because a phone is seized during a lawful arrest. Further, the seizure and search of cell-phone data pursuant to a warrant does not extinguish an otherwise reasonable expectation of privacy in the entirety of the seized data. Rather, a warrant authorizing the police to seize and search cell-phone data allows officers to examine the seized data only to the extent reasonably consistent with the scope of the warrant. In this case, the warrant authorized officers to search defendant's cell-phone data for evidence of drug trafficking as described by the warrant and affidavit. Any further review of the data beyond the scope of the warrant constituted a search that was presumptively invalid under the Fourth Amendment.

2. In considering the Fourth Amendment's requirements for a search of digital data authorized by a warrant, as with any other search conducted pursuant to a warrant, a search of digital data must be reasonably directed at uncovering evidence of the criminal activity alleged in the warrant. Any search that is directed instead toward finding evidence of other, unrelated criminal activity is beyond the scope of the warrant. Under the Fourth Amendment, a warrant must state with particularity not only the items to be searched and seized, but also the alleged criminal activity justifying the warrant. Although the prosecutor argued that the search for evidence of armed robbery fell within the scope of the warrant because the warrant authorized officers to review the entire report that represented the totality of defendant's cell-phone data, the warrant authorized a search of the data for evidence of drug trafficking, not armed robbery. Moreover, the affidavit supporting the warrant did not even mention armed robbery, let alone seek to establish probable cause that defendant committed that offense. While officers are not required, when executing a search of digital data, to review only digital content that a suspect has identified as pertaining to criminal activity, neither is it always reasonable for an officer to review the entirety of the seized digital data on the basis that incriminating information could conceivably be found anywhere on the device. Accordingly, an officer's search of seized digital data must be reasonably directed toward finding evidence of the criminal activity identified in the warrant. In this case, about a month after officers searched defendant's digital data for evidence of drug trafficking, the

prosecutor in the armed-robbery case asked a detective to conduct a focused search of the data for terms pertaining to the armed-robbery case. There was no evidence that a search for these terms would uncover evidence relating to defendant's drug-trafficking activity, nor was there any evidence that defendant hid or manipulated his data to conceal evidence related to drug trafficking. Therefore, the second search of the data was not reasonably directed toward obtaining evidence of drug trafficking and exceeded the scope of the warrant. Accordingly, the second review of the data constituted a warrantless search that violated the Fourth Amendment, and the case had to be remanded to the Court of Appeals for that Court to reconsider defendant's claim of ineffective assistance of counsel and to determine whether defendant was entitled to relief.

Reversed and remanded.

Justice VIVIANO, concurring, agreed with the majority that the second search of defendant's cell-phone data was unlawful under the Fourth Amendment but wrote separately to emphasize his view that a law enforcement officer's subjective intent when searching seized digital data should be included as a potentially dispositive factor when a court considers whether a search was reasonably directed at finding evidence of the criminal activity identified in the warrant. Justice VIVIANO argued that if the search was purposefully conducted to obtain evidence of a crime other than the one identified in the warrant, a court could not conclude that the search was reasonably directed at uncovering evidence of the criminal activity alleged in the warrant. In this case, Justice VIVIANO would find this factor dispositive since it was clear that the second search of defendant's cell-phone data was conducted to obtain evidence of a crime other than drug trafficking, the offense identified in the warrant. Therefore, before conducting the second search of defendant's cell phone, the officer should have obtained a second search warrant directed toward obtaining evidence of the armed-robbery offense. Because he did not, the second search was unlawful.

# OPINION

Chief Justice:  
Bridget M. McCormack

Chief Justice Pro Tem:  
David F. Viviano

Justices:  
Stephen J. Markman  
Brian K. Zahra  
Richard H. Bernstein  
Elizabeth T. Clement  
Megan K. Cavanagh

---

FILED December 28, 2020

STATE OF MICHIGAN

SUPREME COURT

PEOPLE OF THE STATE OF MICHIGAN,

Plaintiff-Appellee,

v

No. 158652

KRISTOPHER ALLEN HUGHES,

Defendant-Appellant.

---

BEFORE THE ENTIRE BENCH

MARKMAN, J.

The issue presented here is whether, when the police obtain a warrant to search digital data from a cell phone for evidence of a crime, they are later permitted to review that same data for evidence of another crime without obtaining a second warrant. We conclude-- in light of the particularity requirement embodied in the Fourth Amendment and given meaning in the United States Supreme Court's decision in *Riley v California*, 573 US 373; 134 S Ct 2473; 189 L Ed 2d 430 (2014) (addressing the "sensitive" nature of cell-phone data)-- that a search of digital cell-phone data pursuant to a warrant must be

reasonably directed at obtaining evidence relevant to the criminal activity alleged in *that* warrant. Any search of digital cell-phone data that is not so directed, but instead is directed at uncovering evidence of criminal activity not identified in the warrant, is effectively a warrantless search that violates the Fourth Amendment absent some exception to the warrant requirement. Here, the officer's review of defendant's cell-phone data for incriminating evidence relating to an armed robbery was not reasonably directed at obtaining evidence regarding drug trafficking-- the criminal activity alleged in the warrant-- and therefore the search for that evidence was outside the purview of the warrant and thus violative of the Fourth Amendment. Accordingly, we reverse the judgment of the Court of Appeals and remand to that Court to determine whether defendant is entitled to relief based upon the ineffective assistance of counsel.<sup>1</sup>

## I. FACTS & HISTORY

The circumstances of this case arise from concurrent criminal prosecutions against defendant Kristopher Hughes, one related to drug trafficking and the other related to armed robbery. MCL 750.529. Defendant pleaded no contest to the drug-trafficking charges and

---

<sup>1</sup> Because we conclude that the Fourth Amendment was breached when officers searched a cell phone for evidence of *armed robbery* without having obtained a second warrant when the phone had been seized based upon a warrant for *drug trafficking*, we need not decide (a) whether the warrant affidavit sufficiently connected defendant's cell phone to his drug trafficking or (b) the broader question as to what evidence set forth in an affidavit sufficiently connects a cell phone to alleged criminal activity to support the issuance of a warrant to search the phone's digital contents. We only address the proper manner of searching digital data when such data has been seized pursuant to a valid warrant.

these pleas are not the subject of this appeal.<sup>2</sup> Defendant went to trial on the armed-robbery charge, and after two mistrials due to hung juries, he was convicted of the armed robbery of Ronald Stites.

On August 6, 2016, Stites was going for a walk when he met Lisa Weber. The two talked, and Stites invited Weber back to his home. At Stites's residence, Weber offered to stay with Stites all night and to perform sexual acts in exchange for \$50. Stites agreed, and Weber followed him into his bedroom, where he opened a safe containing \$4,200 in cash and other items and pulled out a \$50 bill that he agreed to give her after the night was over. Stites then performed oral sex on Weber. Afterward, Weber went to the store to get something to drink. Approximately 15–20 minutes later, she called a drug dealer, who went by the name of "K-1" or "Killer," and asked that he come over and sell drugs to her and Stites. Sometime thereafter, a man arrived at Stites's home, sold Weber and Stites crack cocaine, and then departed. Weber and Stites consumed some of the drugs and continued their sexual activities. Later in the evening, the man who had sold the drugs returned to the home with a gun and stole Stites's safe at gunpoint. Stites testified that Weber assisted in the robbery and departed the home with the robber, while Weber asserted

---

<sup>2</sup> On February 2, 2017, defendant pleaded no contest to two counts of delivery and manufacture of a controlled substance, second or subsequent offense, MCL 333.7401(2)(b)(ii), possession of marijuana, MCL 333.7403(2)(d), possession of suboxone, MCL 333.7403(2)(b)(ii), possession of alprazolam, MCL 333.7403(2)(b)(ii), and possession of dihydrocodeine pills, MCL 333.7403(2)(b)(ii), as a habitual fourth offender. He was sentenced to concurrent prison terms of 36 months to 30 years, 12 to 24 months, and 24 months to 15 years. Defendant appealed and the Court of Appeals denied his application for lack of merit. *People v Hughes*, unpublished order of the Court of Appeals, entered September 28, 2017 (Docket No. 339858). Defendant did not seek leave to appeal in this Court.

that she did not assist in the robbery and only complied with the robber's demands to avoid being harmed. Weber identified defendant as the perpetrator, while Stites could not identify defendant as the perpetrator.

On August 11, 2016, Detective Matthew Gorman submitted a warrant affidavit to search defendant's property for evidence related to separate criminal allegations of drug trafficking. Detective Gorman's affidavit included information from a confidential informant that defendant and an associate named Patrick Pankey were dealing drugs. The warrant affidavit also asserted that as a product of Detective Gorman's experience and training, "drug traffickers commonly use electronic equipment to aid them in their drug trafficking activities. This equipment includes, but is not limited to, . . . mobile telephones . . . ." The warrant affidavit contained no information indicating that Weber was involved in defendant's drug trafficking and did not refer to the previous week's armed robbery at Stites's residence.

The district court judge concluded that there was probable cause for the warrant based upon the attached affidavit and thereby issued a warrant authorizing the police to search three residences that were connected with defendant and his vehicle for further evidence of drug trafficking. As relevant here, the warrant provided:

[A]ny cell phones or . . . other devices capable of digital or electronic storage seized by authority of this search warrant shall be permitted to be forensically searched and or manually searched, and any data that is able to be retrieved there from shall be preserved and recorded.

The warrant also contained the following limitation:

Therein to search for, seize, secure, tabulate and make return according to law, the following property and things:

Crack Cocaine, and any other illegally possessed controlled substances; any raw material, product, equipment or drug paraphernalia for the compounding, cutting, exporting, importing, manufacturing, packaging, processing, storage, use or weighing of any controlled substance; proofs of residence, such as but not limited to, utility bills, correspondence, rent receipts, and keys to the premises; proofs as to the identity of unknown suspects such as but not limited to, photographs, certificates, and/or diplomas; prerecorded, illegal drug proceeds and *any records pertaining to the receipt, possession and sale or distribution of controlled substances including but not limited to documents, video tapes, computer disks, computer hard drives, and computer peripherals*; other mail receipts, containers or wrappers; currency, property obtained through illegal activity, financial instruments, safety deposit box keys, money order receipts, bank statements and related records; firearms, ammunition, and all occupants found inside. [Emphasis added.]

On August 12, 2016, police were executing a search at one of the addresses set forth in the warrant when they detained defendant and seized a phone that was on his person. On August 17, 2016, defendant was arraigned on the charge of armed robbery.

On August 23, 2016, Detective Edward Wagrowski performed a forensic examination of the phone that was seized from defendant, and all of its data was extracted using Cellebrite, software used for extracting digital data. Upon extraction, Cellebrite separated and sorted the device's data into relevant categories by, for example, placing all of the photographs together in a single location. The extraction process resulted in a 600-page report of defendant's cell-phone data, which included more than 2,000 call logs, more than 2,900 text messages, and more than 1,000 photographs. Detective Wagrowski testified at trial that Cellebrite enabled police to enter search terms to isolate data from specific phone numbers or that contained specific words or phrases. If there were no contacts between a searched number and the device being searched, the searcher would receive no results and the software would show a blank screen. It is unclear from the record

whether and to what extent the data extracted from the cell phone was reviewed for evidence of defendant's drug trafficking.

A month or so after the initial extraction, at the request of the prosecutor in defendant's armed-robbery case, Detective Wagrowski conducted further searches of the cell-phone data for: (a) contacts with the phone numbers of Weber and Stites and (b) the name "Lisa," variations on the word "killer" (defendant's nickname), and the name "Kris/Kristopher" (defendant's actual name). These searches uncovered 19 calls between defendant and Weber on the night of the robbery and 15 text messages between defendant and Weber between August 5, 2016 and August 10, 2016. Weber's texts to defendant leading up to the robbery included communications indicating where Stites's home was located, that the home was unlocked, and that there was a flat screen TV in the home. Defendant sent texts to Weber on the night of the robbery asking her to "[t]ext me or call me" and to "open the doo[r]." None of the text messages with the words "killer" or "Kris" were from Weber's number. The prosecutor acknowledged that the results of these searches served as evidence at defendant's armed-robbery trials. Defense counsel objected to the admission of this evidence, arguing that it was "not relevant" and "stale," but the trial court overruled his objection.

Defendant's first two trials on the armed-robbery charge resulted in mistrials due to hung juries. A juror note from the first trial explained that the jury was divided and could not reach a verdict because "Mr. Stites was not able to positively ID Mr. Hughes" and "Mrs. Weber's testimony was not credible (according to some) and she was the only one to positively identify Mr. Hughes from that night." Similarly, a juror note from the second trial listing the jurors' concerns about the evidence stated that "100% of Lisa W[eber's]

testimony is untrue” and further noted the “d[i]screpancy of [defendant’s] description by Ron Stites.” At defendant’s third trial, the prosecutor-- while acknowledging that the jury might have “concerns” regarding Weber’s credibility as a “disputed accomplice” to the armed robbery-- argued during both opening and closing statements that the text messages and phone calls discovered on defendant’s cell phone bolstered her testimony and established a link between defendant and the armed robbery. The jury at defendant’s third trial convicted him of armed robbery, and he was sentenced to 25 to 60 years in prison.

Defendant appealed his conviction, arguing in relevant part that (a) the phone records should have been excluded from trial because the warrant supporting a search of the data only authorized a search for evidence of drug trafficking and not armed robbery and (b) trial counsel had been ineffective in failing to object to the data’s admission under the Fourth Amendment. The Court of Appeals rejected these arguments and affirmed defendant’s conviction. *People v Hughes*, unpublished per curiam opinion of the Court of Appeals, issued September 25, 2018 (Docket No. 338030). Defendant then sought leave to appeal in this Court, and we ordered oral argument on the application. *People v Hughes*, 505 Mich 855 (2019).<sup>3</sup>

---

<sup>3</sup> The Court asked the parties to address specifically:

- (1) whether the probable cause underlying the search warrant issued during the prior criminal investigation authorized police to obtain all of the defendant’s cell phone data;
- (2) whether the defendant’s reasonable expectation of privacy in his cell phone data was extinguished when the police obtained the cell phone data in a prior criminal investigation;
- (3) if not, whether the search of the cell phone data in the instant case was within the scope of the probable cause underlying the search warrant issued during the prior criminal investigation;
- (4) if not, whether the search of the cell phone data in the instant case was lawful; and
- (5) whether trial counsel was

## II. STANDARD OF REVIEW

Questions of constitutional law are reviewed de novo. *People v Hall*, 499 Mich 446, 452; 884 NW2d 561 (2016). Defendant did not object to the admission of the evidence from his cell phone under the Fourth Amendment, so this issue is unpreserved. See *People v Kimble*, 470 Mich 305, 309; 684 NW2d 669 (2004). Unpreserved constitutional claims are reviewed for plain error. *People v Carines*, 460 Mich 750, 764; 597 NW2d 130 (1999).<sup>4</sup> Defendant does not argue that he is entitled to relief under this standard but rather argues that trial counsel was ineffective for failing to object under the Fourth Amendment. The standards for “plain error” review and ineffective assistance of counsel are distinct, and therefore, a defendant can obtain relief for ineffective assistance of counsel even if he or she cannot demonstrate plain error. See generally *People v Randolph*, 502 Mich 1; 917 NW2d 249 (2018).

## III. ANALYSIS

### A. FOURTH AMENDMENT

The Fourth Amendment of the United States Constitution provides:

---

ineffective for failing to challenge the search of the cell phone data in the instant case on Fourth Amendment grounds. [*People v Hughes*, 505 Mich 855 (2019).]

<sup>4</sup> “To avoid forfeiture under the ‘plain error’ rule, three requirements must be met: 1) error must have occurred, 2) the error was plain, i.e., clear or obvious, 3) and the plain error affected substantial rights.” *Carines*, 460 Mich at 763. If these requirements are satisfied, a court must exercise its discretion and should reverse only if the “forfeited error resulted in the conviction of an actually innocent defendant or when an error seriously affected the fairness, integrity or public reputation of judicial proceedings independent of the defendant’s innocence.” *Id.* (quotation marks and brackets omitted).

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. [US Const, Am IV.]<sup>5</sup>

As indicated by the Fourth Amendment’s text, “reasonableness is always the touchstone of Fourth Amendment analysis.” *Birchfield v North Dakota*, 579 US \_\_\_, \_\_\_; 136 S Ct 2160, 2186; 195 L Ed 2d 560 (2016). Thus, a search warrant is not always required before searching or seizing a citizen’s personal effects. See, e.g., *Brigham City v Stuart*, 547 US 398, 403; 126 S Ct 1943; 164 L Ed 2d 650 (2006). However, there is a “strong preference for searches conducted pursuant to a warrant,” *Illinois v Gates*, 462 US 213, 236; 103 S Ct

---

<sup>5</sup> Similarly, the Michigan Constitution has provided:

The person, houses, papers and possessions of every person shall be secure from unreasonable searches and seizures. No warrant to search any place or to seize any person or things shall issue without describing them, nor without probable cause, supported by oath or affirmation. . . . [Const 1963, art 1, § 11.]

This provision was recently amended to explicitly protect “electronic data.” See Graham, Michigan Radio, *Election 2020: Michigan Voters Approve Proposal 2, Protecting Electronic Data* <<https://www.michiganradio.org/post/election-2020-michigan-voters-approve-proposal-2-protecting-electronic-data>> (posted November 4, 2020) (accessed November 6, 2020) [<https://perma.cc/54KC-6XJY>]; 2020 Enrolled Senate Joint Resolution G. “In interpreting our Constitution, we are not bound by the United States Supreme Court’s interpretation of the United States Constitution, even where the language is identical.” *People v Goldston*, 470 Mich 523, 534; 682 NW2d 479 (2004). However, we have recognized that, at least before its recent amendment, the Michigan Constitution generally has afforded the same protections as those secured by the Fourth Amendment. *People v Slaughter*, 489 Mich 302, 311; 803 NW2d 171 (2011). This is true even though the Michigan Constitution since 1936 has contained an express limitation on the application of the exclusionary rule to violations of Article 1, Section 11. See *Goldston*, 470 Mich at 535 n 8. Defendant, however, has not argued that the Michigan Constitution affords greater protections than the Fourth Amendment in the present context, and therefore our analysis here does not address the recent amendment.

2317; 76 L Ed 2d 527 (1983), and the general rule is that officers must obtain a warrant for a search to be reasonable under the Fourth Amendment. See, e.g., *Riley*, 573 US at 382.

In *Riley v California*, the Supreme Court of the United States held that officers must generally obtain a warrant before conducting a search of cell-phone data. *Riley*, 573 US at 386. In so holding, the Court rejected, with respect to cell-phone data, application of the “search incident to a lawful arrest” exception to the warrant requirement, which generally allows police to search and seize items (including closed containers) located on a person during a lawful arrest. *Id.* at 382-386; *United States v Robinson*, 414 US 218, 234-236; 94 S Ct 467; 38 L Ed 2d 427 (1973). The Court reasoned that the justifications provided in *Chimel v California*, 395 US 752, 762-763; 89 S Ct 2034; 23 L Ed 2d 685 (1969), for this exception to the warrant requirement-- potential harm to officers and the destruction of evidence-- are less compelling in the context of digital data. *Riley*, 573 US at 386.

The Court also noted that a “search incident to a lawful arrest” is justified, at least in part, by “an arrestee’s reduced privacy interests upon being taken into police custody.” *Id.* at 391. However, it rejected the proposition that an arrestee loses all expectation of privacy, asserting that “when ‘privacy-related concerns are weighty enough’ a ‘search may require a warrant, notwithstanding the diminished expectations of privacy of the arrestee.’ ” *Id.* at 392, quoting *Maryland v King*, 569 US 435, 463; 133 S Ct 1958; 186 L Ed 2d 1 (2013). The Court held that a warrant was required to search the contents of a cell phone seized during a lawful arrest notwithstanding this reduced expectation of privacy because “[c]ell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee’s person”:

[I]t is no exaggeration to say that many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate. Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case.

Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different. An Internet search and browsing history, for example, can be found on an Internet-enabled phone and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD. Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.

Mobile application software on a cell phone, or “apps,” offer a range of tools for managing detailed information about all aspects of a person's life. There are apps for Democratic Party news and Republican Party news; apps for alcohol, drug, and gambling addictions; apps for sharing prayer requests; apps for tracking pregnancy symptoms; apps for planning your budget; apps for every conceivable hobby or pastime; apps for improving your romantic life. There are popular apps for buying or selling just about anything, and the records of such transactions may be accessible on the phone indefinitely. There are over a million apps available in each of the two major app stores; the phrase “there's an app for that” is now part of the popular lexicon. The average smart phone user has installed 33 apps, which together can form a revealing montage of the user's life. [*Riley*, 573 US at 393, 395-396 (quotation marks and citations omitted).]

*Riley* makes clear that, in light of the extensive privacy interests at stake, general Fourth Amendment principles apply with equal force to the digital contents of a cell phone. See *id.* at 396-397 (“[A] cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.”).

With this constitutional background in mind, the issue posed in this case is whether officers violated the Fourth Amendment when they searched defendant’s cell-phone data in pursuit of evidence that defendant committed an armed robbery when the phone was seized pursuant to a warrant authorizing the search of this data for evidence of unrelated drug trafficking.<sup>6</sup> The prosecutor makes two principal arguments in support of the officer’s search of defendant’s cell-phone data for evidence of the armed robbery: (a) the warrant to seize and search defendant’s cell-phone data for evidence of drug trafficking extinguished

---

<sup>6</sup> Defendant also argues that the district court judge lacked probable cause to authorize the search and seizure of his cell-phone data for evidence of drug trafficking because the probable cause underlying the warrant failed to establish the required nexus between his alleged criminal activity and his cell phone. See *Warden, Maryland Penitentiary v Hayden*, 387 US 294, 307; 87 S Ct 1642; 18 L Ed 2d 782 (1967). He contends that Detective Gorman’s opinion, grounded in his training and expertise, that drug traffickers commonly use cell phones to aid in their criminal enterprise was insufficient to provide probable cause that his cell phone would contain evidence of drug trafficking. Cf. *United States v Brown*, 828 F3d 375, 384 (CA 6, 2016) (“[I]f the affidavit fails to include facts that directly connect the residence with the suspected drug dealing activity, . . . it cannot be inferred that drugs will be found in the defendant’s home—even if the defendant is a known drug dealer.”). In light of the pervasiveness of modern cell-phone use recognized by *Riley*, defendant thus raises a not-unreasonable concern as to the issuance of a warrant to search and seize cell-phone data based solely on the nature of the crime alleged. See *Riley*, 573 US at 399 (“It would be a particularly inexperienced or unimaginative law enforcement officer who could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone.”). On the other hand, there is caselaw to suggest that allegations of drug trafficking are distinct from other alleged criminal activities because cell phones are well-recognized tools of the trade for drug traffickers. See, e.g., *United States v Hathorn*, 920 F3d 982, 985 (CA 5, 2019) (“Cell phones, computers, and other electronic devices are vital to the modern-day drug trade.”). Because we conclude that the officer here violated the Fourth Amendment when he searched defendant’s cell-phone data for evidence of armed robbery without having obtained a second warrant, we need not decide whether the warrant affidavit provided a sufficient nexus between defendant’s drug trafficking and his cell phone. More specifically, we need not decide whether cell phones constitute tools of the trade for drug traffickers such that an affidavit that establishes probable cause of drug trafficking necessarily establishes the required nexus between a suspect’s cell phone and the alleged criminal activity.

defendant's reasonable expectation of privacy in all of his data and therefore no search occurred under the Fourth Amendment and (b) the search for evidence of the armed robbery fell within the scope of the warrant issued to search for evidence of drug trafficking because the warrant authorized officers to review all of defendant's data for evidence of drug trafficking and Weber allegedly bought drugs from defendant before the armed robbery. We respectfully find neither argument persuasive.

### 1. EXPECTATION OF PRIVACY

The first issue is whether defendant lost the reasonable expectation of privacy in his cell-phone data when the cell phone was seized and the data was searched pursuant to the warrant issued in the drug-trafficking case. As this Court has explained:

A search for Fourth Amendment purposes occurs only when “an expectation of privacy that society is prepared to consider reasonable is infringed.” *United States v Jacobsen*, 466 US 109, 113; 104 S Ct 1652; 80 L Ed 2d 85 (1984). “If the inspection by police does not intrude upon a legitimate expectation of privacy, there is no ‘search’ subject to the Warrant Clause.” *Illinois v Andreas*, 463 US 765, 771; 103 S Ct 3319; 77 L Ed 2d 1003 (1983). If a person has no reasonable expectation of privacy in an object, a search of that object for purposes of the Fourth Amendment cannot occur. [*Minnesota v Dickerson*, 508 US 366, 375; 113 S Ct 2130; 124 L Ed 2d 334 (1993)]; *People v Brooks*, 405 Mich 225, 242; 274 NW2d 430 (1979). [*People v Custer*, 465 Mich 319, 333; 630 NW2d 870 (2001).]

It is clear that under *Riley*, citizens maintain a reasonable expectation of privacy in their cell-phone data and this reasonable expectation of privacy does not altogether dissipate merely because a phone is seized during a lawful arrest. The question here is whether the seizure and search of cell-phone data pursuant to a warrant extinguishes that otherwise reasonable expectation of privacy in the entirety of that seized data. We conclude that it does not. Rather, a warrant authorizing the police to seize and search cell-phone data

allows officers to examine the seized data only to the extent reasonably consistent with the scope of the warrant.

The prosecutor argues the seizure of defendant's cell-phone data pursuant to the search warrant eliminated his reasonable expectation of privacy in that data, permitting officers to review all such data without implicating the Fourth Amendment. This argument "overlooks the important difference between searches and seizures." *Horton v California*, 496 US 128, 133; 110 S Ct 2301, 2306; 110 L Ed 2d 112 (1990). "A search compromises the individual interest in privacy; a seizure deprives the individual of dominion over his or her person or property." *Id.* The authority to seize an item does not necessarily eliminate one's expectation of privacy in that item and therefore allow the police to search that item without limitation. See *Jacobsen*, 466 US at 114 ("Even when government agents may lawfully seize . . . a package to prevent loss or destruction of suspected contraband, the Fourth Amendment requires that they obtain a warrant before examining the contents of such a package."); *United States v Chadwick*, 433 US 1, 13 n 8; 97 S Ct 2476; 53 L Ed 2d 538 (1977) ("[T]he [lawful] seizure [of respondents' footlocker] did not diminish respondents' legitimate expectation that the footlocker's contents would remain private."); *Custer*, 465 Mich at 342 ("[W]e do not conclude that, once the police lawfully seize an object from an individual, that individual's reasonable expectation of privacy in that object is altogether lost.") (emphasis omitted). This distinction was also implicitly recognized in *Riley* when the Court held that officers could *seize* a cell phone on a person incident to a lawful arrest but they could not *search* the contents of that phone without a warrant. *Riley*, 573 US at 388, 401. While it may have been reasonable for officers to seize all of defendant's cell-phone data pursuant to the warrant to prevent the destruction of evidence

and to isolate incriminating material from nonincriminating material, it was not necessarily reasonable for police to review that data without limitation.

The prosecutor's reliance on cases holding that a suspect loses all expectation of privacy in items seized from his person during a lawful arrest is inapt. The prosecutor cites *United States v Edwards*, 415 US 800, 801-802, 806; 94 S Ct 1234; 39 L Ed 2d 771 (1974), in which the Supreme Court held that the search and seizure of a suspect's clothes the morning after his arrest was reasonable. The Court recognized that officers could have searched and seized the clothes the defendant wore at the time of his arrest immediately after the arrest and held that a reasonable delay in doing so did not render the search and seizure unreasonable. *Id.* at 805. The Court further commented, "[I]t is difficult to perceive what is unreasonable about the police's examining and holding as evidence those personal effects of the accused that they already have in their lawful custody as the result of a lawful arrest." *Id.* at 806. Relying on *Edwards*, some courts have held that an arrestee lacks any reasonable expectation of privacy in items seized during a lawful arrest and therefore a later examination of those items, even for evidence of a crime other than the crime of arrest, is not a search under the Fourth Amendment. See, e.g., *Wallace v State*, 373 Md 69, 90-94; 816 A2d 883 (2003).

These cases are inapplicable here, as *Riley* distinguished cell-phone data from other items subject to a search incident to a lawful arrest in terms of the privacy interests at stake. See *Riley*, 573 US at 393. *Riley* thus stands for the proposition that seizure of a phone and its digital contents-- unlike a seizure of other items on a person-- does not entirely extinguish one's right to privacy in that data. Moreover, *Edwards* itself did not hold that the mere fact an item was lawfully seized eliminated a suspect's reasonable expectation of

privacy; rather, it recognized that a lawful search of an item on an arrestee's person immediately after arrest was *already* reasonable under the exception to the warrant requirement for searches incident to a lawful arrest and that a reasonable delay in conducting that permissible search did not render the search unreasonable. *Edwards*, 415 US at 805. In other words, the police “did no more [at the police station] than they were entitled to do incident to the usual custodial arrest and incarceration.” *Id.* Thus, assuming that this caselaw is pertinent in the instant context, it reinforces our conclusion that the later review of defendant's cell-phone data for evidence of an armed robbery was only lawful if this review was permissible in the first instance, i.e., if it was within the scope of the warrant issued to search for evidence of drug trafficking. See *State v Betterley*, 191 Wis 2d 406, 418; 529 NW2d 216 (1995) (holding that, based on *Edwards*, “the permissible extent of the second look [at items seized by police incident to a lawful arrest] is defined by what the police could have lawfully done without violating the defendant's reasonable expectations of privacy during the first search, even if they did not do it at that time”).

The prosecutor also argues that because the search warrant authorized officers to search defendant's cell-phone data for evidence of drug trafficking, defendant no longer had a reasonable expectation of privacy in all of his data. Both the prosecutor and the Court of Appeals relied on *United States v Jacobsen* for the proposition that defendant lost all expectation of privacy in his cell-phone data when the search warrant authorized a search of that data for drug trafficking. In *Jacobsen*, the employees of a private freight carrier opened a damaged package and discovered a long tube. *Jacobsen*, 466 US at 111. The employees cut open the tube and discovered plastic bags filled with a white powdery substance. *Id.* The employees summoned a federal agent who, without obtaining a

warrant, removed the bags from the tube, took a small amount of the powder out of the bags, and tested the powder to determine whether it was cocaine. *Id.* at 111-112. The Court noted that a private party’s search of an item does not implicate the Fourth Amendment and held that “[t]he agent’s viewing of what a private party had freely made available for his inspection did not violate the Fourth Amendment.” *Id.* at 119-120. The Court explained:

Once frustration of the original expectation of privacy occurs, the Fourth Amendment does not prohibit governmental use of the now nonprivate information. . . . The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated. [*Id.* at 117.]

Accordingly, the Court held that “[t]he additional invasions of respondents’ privacy by the Government agent must be tested by the degree to which they exceeded the scope of the private search.” *Id.* at 115. The Court concluded that the agent’s removal of the plastic bags from the tube and his visual inspection of the contents of the bags “infringed no legitimate expectation of privacy and hence was not a ‘search’ within the meaning of the Fourth Amendment” because this action did not enable the officer to learn anything that had not previously been uncovered during the private search. *Id.* at 120.<sup>7</sup>

---

<sup>7</sup> *Jacobsen* proceeded to consider aspects of the officer’s actions that exceeded the scope of the private search: the seizure of the plastic bags containing white powder and the testing of the white powder to determine whether it was cocaine. The Court held that the removal of the plastic bags from the box constituted a seizure because the officer had asserted “dominion and control over the package and its contents,” *id.* at 120, but that the seizure nonetheless was reasonable under the Fourth Amendment because “it was apparent that the tube and plastic bags contained contraband and little else.” *Id.* at 121-122. It further held that testing the powder did not constitute a search because the test “merely disclose[d] whether or not [the] particular substance [was] cocaine.” *Id.* at 123. However, the Court noted that the test of the powder involved destruction of some of that powder and that this

*Jacobsen*, in our judgment, does not advance the prosecutor’s argument. *Jacobsen* addressed the degree to which a private party’s search of otherwise private items permits the state to review those items. But there was no private search here. While *Jacobsen* is consistent with the general proposition that one lacks a legitimate expectation of privacy in items that are exposed publicly, see, e.g., *Katz v United States*, 389 US 347, 351; 88 S Ct 507; 19 L Ed 2d 576 (1967), it says little about the extent to which the search of an item pursuant to a search warrant eliminates a citizen’s legitimate expectation of privacy.<sup>8</sup> The prosecutor cites no caselaw indicating that the issuance of a warrant eliminates entirely one’s reasonable expectation of privacy in the place or property to be searched.<sup>9</sup> To the contrary, it is well established that a search warrant allows the state to examine property only to the extent authorized by the warrant. See, e.g., *Bivens v Six Unknown Named Agents of Fed Bureau of Narcotics*, 403 US 388, 394 n 7; 91 S Ct 1999; 29 L Ed 2d 619

---

deprivation of the defendant’s possessory interest constituted a seizure under the Fourth Amendment. *Id.* at 124-125. The Court concluded that this seizure was reasonable because it had a *de minimis* impact on defendant’s property interest and that “the suspicious nature of the material made it virtually certain that the substance tested was in fact contraband.” *Id.* at 125.

<sup>8</sup> Moreover, the other searches and seizures in *Jacobsen*-- specifically, the officer’s reexamination of the contents of the package and seizure of the plastic bags, as well as the field test to determine whether the seized substance was cocaine-- have no analogue in the instant case. The search here did not merely duplicate the previous search, and there was no simple test performed to determine whether the data confirmed illegal activity.

<sup>9</sup> Indeed, the prosecutor cites no caselaw indicating that the issuance of a search warrant eliminates *at all* one’s reasonable expectation of privacy in the items to be searched rather than merely permitting officers *temporarily* to compromise that reasonable expectation of privacy. We need not resolve this semantic difference here because, regardless of how it is framed, the result would be the same-- a warrant only permits police to review an item or area to the extent that such review lies within the scope of the warrant.

(1971) (“[T]he Fourth Amendment confines an officer executing a search warrant strictly within the bounds set by the warrant.”). “If the scope of the search exceeds that permitted by the terms of a validly issued warrant . . . , the subsequent seizure is unconstitutional without more.” *Horton*, 496 US at 140. Thus, a search conducted pursuant to a search warrant-- unlike a private search-- is necessarily limited to the scope of the warrant.

To the extent that *Jacobsen* is relevant in the present context, its reasoning further reinforces our conclusion that the issuance of a search warrant does not eliminate entirely one’s reasonable expectation of privacy but only allows a search consistent with the scope of the warrant. As the United States Court of Appeals for the Sixth Circuit explained in applying *Jacobsen* to the search of a laptop, “[f]or the review of [the defendant’s] laptop to be permissible, *Jacobsen* instructs us that [the officer’s] search had to stay within the scope of [the] initial private search.” *United States v Lichtenberger*, 786 F3d 478, 488 (CA 6, 2015). The court therefore concluded that the officer’s search exceeded the scope of the warrant because there was “no virtual certainty that [the officer’s] review [of the defendant’s digital data] was limited to the photographs from” the earlier private search. *Id.*; see also *United States v Sparks*, 806 F3d 1323, 1336 (CA 11, 2015) (“While [the] private search of the cell phone might have removed certain information from the Fourth Amendment’s protections, it did not expose every part of the information contained in the cell phone.”), overruled on other grounds by *United States v Ross*, 963 F3d 1056 (CA 11, 2020); *State v Terrell*, 372 NC 657, 669, 670; 831 SE2d 17 (2019) (“We cannot agree that the mere opening of a thumb drive and the viewing of as little as one file automatically renders the entirety of the device’s contents ‘now nonprivate information’ no longer [to be] afforded any protection by the Fourth Amendment. . . . [T]he extent to which an

individual's expectation of privacy in the contents of an electronic storage device is frustrated depends upon the extent of the private search and the nature of the device and its contents.”).<sup>10</sup> As applied to the instant situation, under *Jacobsen*, the scope of the officer's search of defendant's data for evidence of armed robbery was limited to the scope of the initial lawful intrusion, i.e., the breadth of the warrant in the drug-trafficking case. Accordingly, *Jacobsen* does not support the proposition that defendant lost entirely his expectation of privacy in all of his cell-phone data once the cell phone was seized and the data searched pursuant to a warrant.<sup>11</sup>

---

<sup>10</sup> At least two federal courts of appeals have held that under *Jacobsen*, once there is a private search of any part of a suspect's digital data, police officers are permitted to review all the data on that device without a warrant, comparing digital data to a closed container that when opened loses all expectation of privacy. *United States v Runyan*, 275 F3d 449, 464 (CA 5, 2001); *Rann v Atchison*, 689 F3d 832, 836-837 (CA 7, 2012). For the reasons stated below, we find unpersuasive, in light of the United States Supreme Court's subsequent decision in *Riley*, the analogy of a digital device to a closed container and thus find these cases unpersuasive.

<sup>11</sup> While not cited by the prosecutor, we recognize that the Minnesota Court of Appeals in *State v Johnson*, 831 NW2d 917, 924 (Minn App, 2013), reached the opposite conclusion to that we reach here, holding that “the execution of the warrant ‘frustrated’ and terminated appellant's expectation of privacy in the hard drive and the digital contents identified in the warrant.” *Johnson* relied on *Illinois v Andreas*, in which the United States Supreme Court held that “the subsequent reopening of [a] container is not a ‘search’ within the intendment of the Fourth Amendment” and that “absent a substantial likelihood that the contents have been changed, there is no legitimate expectation of privacy in the contents of a container previously opened under lawful authority.” *Andreas*, 463 US at 772-773. However, *Andreas*'s holding regarding the opening of a closed container, as with those holdings cited in note 10 of this opinion, is also inapplicable to searches of cell-phone data in light of *Riley*'s subsequent recognition that privacy interests in digital data may greatly exceed those with regard to more mundane physical objects. *Riley*, 573 US at 393, 397 (holding that comparing a search of physical objects to a search of digital data is “like saying a ride on horseback is materially indistinguishable from a flight to the moon,” and noting that “[t]reating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained”). See also Kerr, *Searches and Seizures in A Digital World*,

In summary, the search and seizure of defendant’s cell-phone data pursuant to a warrant in the drug-trafficking case did not altogether eliminate his reasonable expectation of privacy in that data. Rather, the police were permitted to seize and search that data, but only to the extent authorized by the warrant. Any further review of the data beyond the scope of that warrant constitutes a search that is presumptively invalid under the Fourth Amendment, absent some exception to that amendment’s warrant requirement. See *Horton*, 496 US at 140. The remaining question is whether the review of defendant’s data for evidence of an armed robbery fell within the scope of the warrant issued in the drug-trafficking case.

## 2. SCOPE OF THE WARRANT

This Court has yet to specifically address the Fourth Amendment requirements for a search of digital data from a cell phone authorized by a warrant. In considering this issue, we are guided by two fundamental sources of relevant law: (a) the Fourth Amendment’s “particularity” requirement, which limits an officer’s discretion when conducting a search pursuant to a warrant and (b) *Riley*’s recognition of the extensive privacy interests in cellular data. In light of these legal predicates, we conclude that as with any other search

---

119 Harv L Rev 531, 555 (2005) (arguing that “[a] computer is like a container that stores thousands of individual containers”). Numerous courts since *Riley* have similarly interpreted that decision, as we believe it must be interpreted, as rejecting an analogy between searches of digital data and searches of closed containers. See, e.g., *Lichtenberger*, 786 F3d at 487 (“[S]earches of physical spaces and the items they contain differ in significant ways from searches of complex electronic devices under the Fourth Amendment.”); *United States v Jenkins*, 850 F3d 912, 920 n 3 (CA 7, 2017); *Terrell*, 372 NC at 669; *United States v Lara*, 815 F3d 605, 610 (CA 9, 2016). Accordingly, we respectfully find *Johnson* to be unpersuasive and decline to adopt its reasoning in light of *Riley*.

conducted pursuant to a warrant, a search of digital data from a cell phone must be “reasonably directed at uncovering” evidence of the criminal activity alleged in the warrant and that any search that is not so directed but is directed instead toward finding evidence of *other* and *unrelated* criminal activity is beyond the scope of the warrant. *United States v Loera*, 923 F3d 907, 917, 922 (CA 10, 2019); see also *Horton*, 496 US at 140-141.

The Fourth Amendment requires that search warrants “particularly describ[e] the place to be searched, and the persons or things to be seized.” US Const, Am IV. A search warrant thus must state with particularity not only the items to be searched and seized, but also the alleged criminal activity justifying the warrant. See *Berger v State of New York*, 388 US 41, 55-56; 87 S Ct 1873; 18 L Ed 2d 1040 (1967); *Andresen v Maryland*, 427 US 463, 479-480; 96 S Ct 2737; 49 L Ed 2d 627 (1976); *United States v Galpin*, 720 F3d 436, 445 (CA 2, 2013) (“[A] warrant must identify the specific offense for which the police have established probable cause.”). That is, some context must be supplied by the affidavit and warrant that connects the particularized descriptions of the venue to be searched and the objects to be seized with the criminal behavior that is suspected, for even particularized descriptions will not always speak for themselves in evidencing criminality. See *Hayden*, 387 US at 307 (“There must, of course, be a nexus . . . between the item to be seized and criminal behavior. Thus . . . , probable cause must be examined in terms of cause to believe that the evidence sought will aid in a particular apprehension or conviction. In so doing, consideration of police purposes will be required.”).

The manifest purpose of this particularity requirement was to prevent general searches. By limiting the authorization to search to the specific areas and things for which there is probable cause to search, the requirement ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers

intended to prohibit. [*Maryland v Garrison*, 480 US 79, 84; 107 S Ct 1013; 94 L Ed 2d 72 (1987); see also, e.g., *Horton*, 496 US at 139.]

While “officers do not have to stop executing a search warrant when they run across evidence outside the warrant’s scope, they must nevertheless reasonably direct their search toward evidence specified in the warrant.” *Loera*, 923 F3d at 920; see also *United States v Ramirez*, 523 US 65, 71; 118 S Ct 992; 140 L Ed 2d 191 (1998) (“The general touchstone of reasonableness . . . governs the method of execution of the warrant.”). For example, a warrant authorizing police to search a home for evidence of a stolen television set would not permit officers to search desk drawers for evidence of drug possession. See *Horton*, 496 US at 140-141.<sup>12</sup> This particularity requirement defines the permissible scope of a search pursuant to a warrant, and any deviation from that scope is a warrantless search that is unreasonable absent an exception to the warrant requirement. *Id.* at 140. More specifically, in connection with the present case the state exceeds the scope of a warrant where a search is not reasonably directed at uncovering evidence related to the criminal activity identified in the warrant, but rather is designed to uncover evidence of criminal activity *not* identified in the warrant. See, e.g., *United States v Carey*, 172 F3d 1268, 1272-

---

<sup>12</sup> As noted by *Riley*, a home and a cell phone are similarly situated, at least to the extent that a search of either may result in a significant intrusion into an individual’s private affairs. *Riley*, 573 US at 396-397 (“In 1926, [Judge] Hand observed . . . that it is ‘a totally different thing to search a man’s pockets and use against him what they contain, [than to] ransack[] his house for everything which may incriminate him.’ If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell-phone search would typically expose to the government far *more* than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.”) (citation omitted).

1273 (CA 10, 1999); *Loera*, 923 F3d at 922; *United States v Nasher-Alneam*, 399 F Supp 3d 579, 593-594 (SD W Va, 2019).

In this regard, we first address the prosecutor’s argument that the search for evidence of armed robbery fell within the scope of the warrant because the warrant authorized officers to review the entire 600-page report containing the apparent totality of defendant’s cell-phone data, as any segment of this data may have contained evidence of drug trafficking and digital data can be manipulated to hide incriminating content.<sup>13</sup> We are cognizant that a criminal suspect will not always store or organize incriminating information on his or her digital devices in the most obvious way or in a manner that

---

<sup>13</sup> Implicit in this argument is the assumption that an officer’s subjective intention to look for evidence related to a crime not identified in the warrant is immaterial so long as the search is objectively authorized by the scope of the warrant. In other words, the prosecutor’s argument seems premised on the proposition that so long as it was objectively reasonable to review *all* of defendant’s data for evidence of drug trafficking, it is irrelevant that the genuine purpose of the search was to secure evidence of an armed robbery. The facts that the prosecutor in the armed-robbery case asked Detective Wagrowski-- a month or so after the initial extraction of the data-- to conduct a further search of defendant’s cell-phone data using search terms related to the armed robbery and that this evidence was eventually admitted in the armed-robbery trials suggests that this search was not designed to obtain evidence related to drug trafficking, but rather to bolster the prosecutor’s case in the armed-robbery trial. Some courts have held that an officer’s subjective intention to find evidence of a crime not identified in the warrant constitutes a relevant factor in determining whether a search of digital data falls outside the scope of the warrant, while others have held that this is a purely objective inquiry. Compare *Loera*, 923 F3d at 919 & n 3 (holding that the subjective intention of the officer to discern evidence of a crime not identified in the warrant is a relevant factor in determining whether the search exceeded the scope of the warrant), with *United States v Williams*, 592 F3d 511, 522 (CA 4, 2010) (“[T]he scope of a search conducted pursuant to a warrant is defined objectively by the terms of the warrant and the evidence sought, not by the subjective motivations of an officer.”) (emphasis omitted). Because the search here was objectively beyond the scope of the warrant, we need not decide whether an officer’s subjective intention is a relevant consideration.

facilitates the location of that information. See, e.g., *United States v Mann*, 592 F 3d 779, 782 (CA 7, 2010) (“Unlike a physical object that can be immediately identified as responsive to the warrant or not, computer files may be manipulated to hide their true contents.”). We do not hold or imply here that officers in the execution of a search of digital data must review only digital content that a suspect deigns to identify as pertaining to criminal activity. See *United States v Burgess*, 576 F3d 1078, 1093-1094 (CA 10, 2009). Such an approach would undermine legitimate law enforcement practices and unduly restrict officers well beyond the dictates of the Fourth Amendment.

However, at the same time, we decline to adopt a rule that it is always reasonable for an officer to review the entirety of the digital data seized pursuant to a warrant on the basis of the mere possibility that evidence may conceivably be found anywhere on the device or that evidence might be concealed, mislabeled, or manipulated. Such a per se rule would effectively nullify the particularity requirement of the Fourth Amendment in the context of cell-phone data and rehabilitate an impermissible *general warrant* that “would in effect give ‘police officers unbridled discretion to rummage at will among a person’s private effects.’ ” *Riley*, 573 US at 399, quoting *Arizona v Gant*, 556 US 332, 345; 129 S Ct 1710; 173 L Ed 2d 485 (2009); see also *People v Herrera*, 357 P3d 1227, 1228, 1233; 2015 CO 60 (Colo, 2015) (holding that allowing a search of an entire device for evidence of a crime based upon the possibility that evidence of the crime could be found anywhere on the phone and that the incriminating data could be hidden or manipulated would “render the warrant a general warrant in violation of the Fourth Amendment’s particularity requirement”). This result would be especially problematic in light of *Riley*’s observations concerning the sheer amount of information contained in cellular data and the highly

personal character of much of that information. *Riley*, 573 US at 394-396; see also *United States v Otero*, 563 F3d 1127, 1132 (CA 10, 2009) (“The modern development of the personal computer and its ability to store and intermingle a huge array of one’s personal papers in a single place increases law enforcement’s ability to conduct a wide-ranging search into a person’s private affairs, and accordingly makes the particularity requirement that much more important.”); *Galpin*, 720 F3d at 447 (“There is . . . a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant. This threat demands a heightened sensitivity to the particularity requirement in the context of digital searches.”) (quotation marks and citation omitted). Accordingly, an officer’s search of seized digital data, as with any other search conducted pursuant to a warrant, must be reasonably directed at finding evidence of the criminal activity identified within the warrant. *Loera*, 923 F3d at 921-922.

Specifically in the digital context, this requires that courts and officers consider “whether the forensic steps of the search process were reasonably directed at uncovering the evidence specified in the search warrant.” *Id.* at 917. Whether a search of seized digital data that uncovers evidence of criminal activity not identified in the warrant was reasonably directed at finding evidence relating to the criminal activity alleged in the warrant turns on a number of considerations, including: (a) the nature of the criminal activity alleged and the type of digital data likely to contain evidence relevant to the alleged activity;<sup>14</sup> (b) the

---

<sup>14</sup> For example, in the absence of contrary case-specific information, it is unlikely that evidence relating to tax fraud would be discovered by reviewing the images on a digital device. See *Carey*, 172 F3d at 1275 n 8 (“Where a search warrant seeks only financial records, law enforcement officers should not be allowed to search through telephone lists or word processing files absent a showing of some reason to believe that these files contain

evidence provided in the warrant affidavit for establishing probable cause that the alleged criminal acts have occurred;<sup>15</sup> (c) whether nonresponsive files are segregated from

---

the financial records sought.”) (quotation marks and citation omitted); Gershowitz, *The Post-Riley Search Warrant: Search Protocols on Particularity in Cell Phone Searches*, 69 *Vanderbilt L Rev* 585, 630-638 (2016) (arguing that criminals engaged in simpler types of street crimes, such as drug trafficking, are more likely to use cell phones and less likely to “mislabel . . . or bury evidence” than criminals engaged in crimes like child pornography and financial misconduct and therefore searches of cell phones for evidence of these simpler crimes should be more limited in scope than searches of computers for evidence of child pornography or financial misconduct).

<sup>15</sup> “The fact that [a warrant] application adequately described the ‘things to be seized’ does not save [a] warrant from its facial invalidity. The Fourth Amendment by its terms requires particularity in the warrant, not in the supporting documents.” *Groh v Ramirez*, 540 US 551, 557; 124 S Ct 1284; 157 L Ed 2d 1068 (2004) (emphasis omitted). However, the particularity requirement of the Fourth Amendment can be satisfied by an affidavit that the warrant incorporates by reference. See, e.g., *United States v Hamilton*, 591 F3d 1017, 1025 (CA 8, 2010). “[M]ost Courts of Appeals have held that a court may construe a warrant with reference to a supporting application or affidavit if the warrant uses appropriate words of incorporation, and if the supporting document accompanies the warrant.” *Groh*, 540 US at 557-558. The prosecutor argues that the warrant here incorporated the warrant affidavit by reference. The warrant stated, “THE ATTACHED AFFIDAVIT, having been sworn to by the affiant, Detective Matthew Gorman, before me this day, based upon facts stated therein, probable cause having been found in the name of the people of the State of Michigan, I command that you enter the following described places and vehicles[.]” The warrant affidavit in this case accompanied the warrant, but it is unclear whether the warrant used “appropriate words of incorporation.” We need not resolve this issue here except to say that regardless of whether a warrant incorporates the affidavit by reference, consideration of the evidence provided in the warrant affidavit for establishing probable cause is relevant to whether a search of digital data was reasonably directed at discovering evidence of the crime alleged in the warrant. Cf. *State v Goynes*, 303 Neb 129, 142; 927 NW2d 346 (2019) (“[A] warrant for the search of the contents of a cell phone must be sufficiently limited in scope to allow a search of only that content that is related to the probable cause that justifies the search.”); Dennis, *Regulating Search Warrant Execution Procedure for Stored Electronic Communications*, 86 *Fordham L Rev* 2993, 3012 (2018) (noting that it is relevant to a search’s reasonableness “whether the government subjected the materials to subsequent searches based on new information and theories developed about the case. In these instances, courts have expressed concern about continued searches for evidence under new theories of the case or more expansive areas not initially included

responsive files on the device;<sup>16</sup> (d) the timing of the search in relation to the issuance of the warrant and the trial for the alleged criminal acts;<sup>17</sup> (e) the technology available to allow officers to sort data likely to contain evidence related to the criminal activity alleged in the warrant from data not likely to contain such evidence without viewing the contents of the unresponsive data and the limitations of this technology;<sup>18</sup> (f) the nature of the digital

---

in the warrant”), citing *United States v Wey*, 256 F Supp 3d 355, 406 (SDNY, 2017); *People v Thompson*, 28 NYS3d 237, 255 (2016).

<sup>16</sup> See *Loera*, 923 F3d at 919.

<sup>17</sup> See *Nasher-Alneam*, 399 F Supp 3d 579 (holding that a second search of digital data for evidence of fraud 15 months after the records were seized to be searched for evidence of distribution of a controlled substance and after the defendant had already gone to trial once exceeded the scope of the warrant); *United States v Metter*, 860 F Supp 2d 205, 209, 211, 215 (EDNY, 2012) (holding that a fifteen-month delay in the government’s review of seized devices violated the Fourth Amendment); *United States v Keszthelyi*, 308 F3d 557, 568-569 (CA 6, 2002) (“[A] single search warrant may authorize more than one entry into the premises identified in the warrant, as long as the second entry is a reasonable continuation of the original search;” “the subsequent entry must indeed be a continuation of the original search, and not a new and separate search.”). But see *United States v Johnston*, 789 F 3d 934, 941-943 (CA 9, 2015) (holding that a search of seized data five years after the initial seizure was reasonable where the search was for evidence of the same criminal conduct alleged in the warrant).

<sup>18</sup> “[L]aw enforcement officers can generally employ several methods to avoid searching files of the type not identified in the warrant: observing files types and titles listed on the directory, doing a key word search for relevant terms, or reading portions of each file stored in the memory.” *Carey*, 172 F3d at 1276; see also Baron-Evans, *When the Government Seizes and Searches Your Client’s Computer*, 18 No. 7 White-Collar Crime Rep 2 (2004); 2004 WL 635186 at 7 (“Various technical means are available to enable the government to confine the search to the scope of probable cause, including searching by filename, directory or subdirectory; the name of the sender or recipient of e-mail; specific key words or phrases; particular types of files as indicated by filename extensions; and/or file date and time.”). The availability of such methods does not necessarily foreclose a more general search of the data. See Perldeiner, *Total Recall: Computers and the Warrant Clause*, 49 Conn L Rev 1757, 1777-1779 (2017) (noting four situations in which searching for and isolating data is difficult: (a) when metadata is deleted, (b) when data is encrypted, (c)

device being searched;<sup>19</sup> (g) the type and breadth of the search protocol employed;<sup>20</sup> (h) whether there are any indications that the data has been concealed, mislabeled, or manipulated to hide evidence relevant to the criminal activity alleged in the warrant, such as when metadata is deleted or when data is encrypted;<sup>21</sup> and (i) whether, after reviewing a certain number of a particular type of data, it becomes clear that certain types of files are not likely to contain evidence related to the criminal activity alleged in the warrant.<sup>22</sup>

---

when data is stored off-site, and (d) when searching for images); see also *Rosa v Commonwealth*, 48 Va App 93, 101; 628 SE2d 92 (2006) (“[F]ile extensions may be misleading and may not give accurate descriptions of the material contained in the file.”). However, the use and availability of such technology is relevant to whether a more general search of the data is reasonable.

<sup>19</sup> See Note, *What Comes After “Get a Warrant”: Balancing Particularity and Practicality in Mobile Device Search Warrants Post-Riley*, 101 Cornell L Rev 187, 204-208 (2015) (arguing that a reasonable search method of cell-phone data will differ from a reasonable search of computer data because “(1) there are different forensic steps involved with mobile device searches compared to computer searches and (2) mobile phones are functionally different from computers”).

<sup>20</sup> “To undertake any meaningful assessment of the government’s search techniques [of digital data], [a court] would need to understand what protocols the government used, what alternatives might have reasonably existed, and why the latter rather than the former might have been more appropriate.” *United States v Christie*, 717 F3d 1156, 1167 (CA 10, 2013). See also *Loera*, 923 F3d at 920.

<sup>21</sup> *Total Recall*, 49 Conn L Rev at 1777-1779; see also *Herrera*, 357 P3d at 1233 (concluding that the “abstract possibility” that files could be hidden or manipulated is insufficient to justify searching the entire phone and noting that the prosecutor “did not present a shred of evidence to suggest, nor did [he] attempt to argue,” that the defendant in that case hid or manipulated his files).

<sup>22</sup> See *Carey*, 172 F3d at 1274 (“[E]ach of the files containing pornographic material was labeled ‘JPG’ and most featured a sexually suggestive title. Certainly after opening the first file and seeing an image of child pornography, the searching officer was aware—in advance of opening the remaining files—what the label meant. When he opened the

To be clear, a court will generally need to engage in such a “totality-of-circumstances” analysis to determine whether a search of digital data was reasonably directed toward finding evidence of the criminal activities alleged in the warrant only if, while searching digital data pursuant to a warrant for one crime, officers discover evidence of a different crime without having obtained a second warrant and a prosecutor seeks to use that evidence at a subsequent criminal prosecution. Courts should also keep in mind that in the process of ferreting out incriminating digital data it is almost inevitable that officers will have to review *some* data that is unrelated to the criminal activity alleged in the authorizing warrant. *United States v Richards*, 659 F3d 527, 539 (CA 6, 2011) (“[O]n occasion in the course of a reasonable search [of digital data], investigating officers may examine, ‘at least cursorily,’ some ‘innocuous documents . . . in order to determine whether they are, in fact, among those papers authorized to be seized.’”), quoting *Andresen*, 427 US at 482 n 11. The fact that some data reviewed turns out to be related to criminal activity not alleged in the authorizing warrant does not render that search per se outside the scope of the warrant. So long as it is reasonable under all of the circumstances for officers to believe that a particular piece of data will contain evidence relating to the criminal activity identified in the warrant, officers may review that data, even if that data ultimately provides evidence of criminal activity not identified in the warrant.

In this case, the warrant authorized officers to search defendant’s digital data for evidence of drug trafficking, or more specifically, for evidence of “any records pertaining

---

subsequent files, he knew he was not going to find items related to drug activity as specified in the warrant . . .”).

to the receipt, possession and sale or distribution of controlled substances including but not limited to documents, video tapes, computer disks, computer hard drives, and computer peripherals.” The affidavit did not even mention Weber or the armed robbery of Stites, let alone seek to establish probable cause that defendant committed armed robbery. As a result, the warrant did not authorize a search of defendant’s data for evidence related to the armed robbery.

A month or so after the initial extraction of the data, the prosecutor in the armed-robbery case asked Detective Wagrowski to use Cellebrite to conduct a focused review of the seized data for (a) contacts with phone numbers of Weber and Stites and (b) data containing the words “Lisa,” “killer” (and variations thereof), and “Kristopher.” The data obtained from this review was admitted into evidence against defendant at his trials for armed robbery.

There was nothing in the warrant or affidavit to suggest that either Weber or Stites was implicated in defendant’s drug trafficking or that reviewing data with Weber’s name or contacts with her phone number would lead to evidence regarding defendant’s drug trafficking. Similarly, there was nothing in the warrant or affidavit to suggest that reviewing defendant’s data for the word “killer” or defendant’s name would uncover evidence of drug trafficking. Furthermore, there was no evidence that defendant hid or manipulated his files to conceal evidence related to his drug trafficking or that a review of all defendant’s data to discover evidence of drug trafficking was reasonable in light of the use and availability of Cellebrite to isolate relevant data. Therefore, this review was not reasonably directed toward obtaining evidence of drug trafficking and exceeded the scope of the warrant.

The prosecutor argues that this review was not beyond the scope of the warrant because defendant allegedly was selling drugs to Weber around the time of the robbery. The prosecutor reasons that defendant's contacts with Weber were rooted in the same illicit activity the warrant had targeted, i.e., drug trafficking. However, any connection between Weber and defendant's drug trafficking was not derived from the warrant or its supportive affidavit. Rather, probable cause that defendant was dealing drugs was based on the tip from a confidential informant that defendant and Pankey were dealing drugs. Therefore, a keyword search of the data for drug references, drug-related items, or contacts with Pankey would certainly have been reasonably directed at finding evidence of drug trafficking and would have fallen well within the scope of the warrant.<sup>23</sup> But there was no indication in the warrant or its affidavit that the review conducted would uncover evidence of defendant's drug trafficking.<sup>24</sup> Rather, the keyword searches were directed toward

---

<sup>23</sup> This list is merely illustrative and is not intended to identify *all* of the potential search terms that would have fallen within the scope of the warrant. Nor is this list intended to imply that officers were only permitted to review defendant's data using search terms rather than employing different search protocols or manually searching the data using other criteria that were reasonably directed in light of the warrant and its affidavit toward finding evidence related to drug trafficking.

<sup>24</sup> We do not mean to hold or imply that police officers are categorically precluded from reviewing cell-phone contacts with a particular person merely because that person has not been explicitly identified in the warrant or supportive affidavit. The evidence set forth for establishing probable cause is but one consideration in determining whether a search of cell-phone data was "reasonably directed" at uncovering evidence related to the crime alleged in the warrant. Therefore, other considerations may well support an officer's review of contacts despite the absence of an express reference to that person in the warrant or affidavit. For example, if, while searching cell-phone data for specific drug-related terms or references used by the defendant, an officer discovers those terms or references within cell-phone contacts, these may of course be reviewed. Further, if an officer were to uncover evidence that digital files containing contacts with a particular person had been

obtaining evidence that defendant committed an armed robbery based on evidence obtained while investigating that armed robbery. Because the warrant did not authorize a search of defendant's data for evidence of armed robbery, these searches fell beyond the scope of the warrant.

To summarize, the officer's review of defendant's cell-phone data for evidence relating to the armed robbery was beyond the scope of the warrant because there was no indication in either the warrant or the affidavit that this review, conducted well after the initial extraction of the data, would uncover evidence of drug trafficking. Additionally, a review of the entirety of defendant's data was unreasonable in light of the lack of evidence that data concerning the drug activity was somehow hidden or manipulated and in light of the officer's ability to conduct a more focused review of the data using Cellebrite to isolate and separate responsive and unresponsive materials. This is not a circumstance in which the officer was reasonably reviewing data for evidence of drug trafficking and happened to view data implicating defendant in other criminal activity. If such were the case and the data's "incriminating character [was] immediately apparent," the plain-view exception would likely apply and permit the state to use the evidence of criminal activity not alleged in the warrant at a subsequent criminal prosecution. *People v Champion*, 452 Mich 92,

---

hidden, manipulated, or encoded in a manner intended to conceal the contacts, the officer might also be justified in suspecting that there was evidence of criminal activity within those contacts regardless of whether that person was referred to in the warrant or affidavit. However, we discern no such considerations in the instant case that would justify the searches of Weber or Stites.

101; 549 NW2d 849 (1996), citing *Horton*, 496 US 128.<sup>25</sup> Rather, this review was directed exclusively toward finding evidence related to the armed-robbery charge, and it was grounded in information obtained during investigation into *that* crime. Accordingly, this review constituted a warrantless search that was unlawful under the Fourth Amendment.<sup>26</sup>

---

<sup>25</sup> The exception is not implicated in this case because “an essential predicate of the plain view doctrine is that the initial intrusion not violate the Fourth Amendment” and the officer’s search here *did* violate the Fourth Amendment because it was not reasonably directed at uncovering evidence of the criminal activities alleged in the warrant. *Galpin*, 720 F3d at 451 (quotation marks omitted); see also *United States v Gurczynski*, 76 MJ 381, 388 (2017) (“A prerequisite for the application of the plain view doctrine is that the law enforcement officers must have been conducting a lawful search when they stumbled upon evidence in plain view. As noted, the officers in this case were not [doing so] because the execution of the warrant was constitutionally unreasonable.”).

<sup>26</sup> Defendant contends the warrant was overly broad because it allowed officers to search his cell phone for evidence of drug trafficking without limitation. In light of the privacy interests implicated in digital data, some magistrates have been placing more specific limitations upon a warrant to search digital data, such as “by (1) instituting time limits on completion [of the search], (2) mandating return or deletion of non-responsive materials, or (3) enumerating specific search protocol to be utilized during execution.” *Regulating Search Warrant Execution*, 86 Fordham L Rev at 3001-3011; see also *In re Search of 3817 W West End, First Floor Chicago, Illinois 60621*, 321 F Supp 2d 953, 961 (ND Ill, 2004) (requiring the government to provide a specific search protocol of digital data to satisfy the particularity requirement of the Fourth Amendment). There is much debate regarding the propriety and constitutionality of ex ante limitations on the manner in which officers may search digital data for evidence. Compare *The Post-Riley Search Warrant*, 69 Vanderbilt L Rev at 638 (“Imposing restrictions on search warrants—in the form of ex ante search protocols and geographic restrictions on the applications police can search—is the best way to ensure that cell phone warrants do not become the reviled general warrants the Fourth Amendment’s particularity requirement was designed to prevent.”), with Kerr, Abstract, *Ex Ante Regulation of Computer Search and Seizure*, 96 Va L Rev 1241, 1242, 1265, 1267-1268 (2010) (“[E]x ante restrictions on the execution of computer warrants are constitutionally unauthorized and unwise.”), citing *United States v Grubbs*, 547 US 90, 98; 126 S Ct 1494; 164 L Ed 2d 195 (2006) (“Nothing in the language of the Constitution or in this Court’s decisions . . . suggests that . . . search warrants . . . must include a specification of the precise manner in which they are to be executed.”) (quotation marks omitted). But see *In re Search Warrant*, 193 Vt 51, 69; 71 A3d 1158 (2012) (holding that,

## B. INEFFECTIVE ASSISTANCE OF COUNSEL

The final issue is whether trial counsel was ineffective when he failed to object under the Fourth Amendment to the admission of the evidence obtained from defendant's cell-phone data. The Court of Appeals rejected out-of-hand defendant's claim of ineffective assistance of counsel based on its conclusion that an objection under the Fourth Amendment would have been futile. *Hughes*, unpub op at 3 n 2. We find it appropriate to remand to the Court of Appeals to reconsider defendant's claim in light of this opinion. When making this determination, the Court of Appeals should consider whether the violation of defendant's Fourth Amendment rights entitled defendant to exclusion of the unlawfully searched data from his armed-robbery trial. See *Kimmelman v Morrison*, 477 US 365, 375; 106 S Ct 2574; 91 L Ed 2d 305 (1986).<sup>27</sup>

---

although *ex ante* restrictions are not required, such restrictions on searches of digital data “are sometimes acceptable mechanisms for ensuring the particularity of a search”). “[G]iven the unique problem encountered in computer searches, and the practical difficulties inherent in implementing universal search methodologies, the majority of federal courts have eschewed the use of a specific search protocol and, instead, have employed the Fourth Amendment’s bedrock principle of reasonableness on a case-by-case basis . . . .” *Richards*, 659 F3d at 538 (citations omitted). We need not decide here whether the warrant was overly broad because “putting aside for the moment the question what limitations the Fourth Amendment’s particularity requirement should or should not impose on the government *ex ante*, the Amendment’s protection against ‘unreasonable’ searches surely allows courts to assess the propriety of the government’s search methods . . . *ex post* in light of the specific circumstances of each case.” *Christie*, 717 F3d at 1166, citing *Ramirez*, 523 US at 71. We conclude that, regardless of whether the warrant itself was overly broad, the search of the data pursuant to that warrant was unreasonable and therefore violated the Fourth Amendment.

<sup>27</sup> The general rule is that evidence obtained in violation of the Fourth Amendment cannot be used against a defendant at a subsequent trial. See, e.g., *United States v Council*, 860 F3d 604, 608-609 (CA 8, 2017); *Mapp v Ohio*, 367 US 643, 655; 81 S Ct 1684; 6 L Ed 2d 1081 (1961) (applying the exclusionary rule to the states). However, the exclusionary rule is a judicially created remedy that does not apply to every Fourth Amendment violation.

#### IV. CONCLUSION

The ultimate holding of this opinion is simple and straightforward-- a warrant to search a suspect's digital cell-phone data for evidence of one crime does not enable a search of that same data for evidence of another crime without obtaining a second warrant. Nothing herein should be construed to restrict an officer's ability to conduct a reasonably thorough search of digital cell-phone data to uncover evidence of the criminal activity alleged in a warrant, and an officer is not required to discontinue a search when he or she discovers evidence of other criminal activity while reasonably searching for evidence of the criminal activity alleged in the warrant. However, respect for the Fourth Amendment's requirement of particularity and the extensive privacy interests implicated by cell-phone data as delineated by the United States Supreme Court's decision in *Riley v California* requires that officers reasonably limit the scope of their searches to evidence related to the criminal activity alleged in the warrant and not employ that authorization as a basis for seizing and searching digital data in the manner of a *general warrant* in search of evidence of any and all criminal activity. We hold that, as with any other search, an officer must limit a search of digital data from a cell phone in a manner reasonably directed to uncover

---

See, e.g., *Utah v Strieff*, 579 US \_\_\_, \_\_\_; 136 S Ct 2056, 2061; 195 L Ed 2d 400 (2016). The prosecutor argues in this Court that if the warrant affidavit failed to establish a sufficient nexus between defendant's criminal activity and his cell phone, see note 6 of this opinion, the exclusionary rule does not apply because the officers relied in good faith on the district court judge's finding of probable cause. See *United States v Leon*, 468 US 897; 104 S Ct 3405; 82 L Ed 2d 677 (1984) (holding that the exclusionary rule does not apply if officers rely in good faith on a magistrate's finding of probable cause to issue a warrant). The prosecutor does not specifically argue that if the searches at issue exceeded the scope of the warrant any exception to the exclusionary rule applies. The parties may develop this issue further on remand.

evidence of the criminal activity alleged in the warrant. We hereby reverse the judgment of the Court of Appeals and remand to that Court to address whether defendant is entitled to relief based upon the ineffective assistance of counsel.

Stephen J. Markman  
Bridget M. McCormack  
Brian K. Zahra  
David F. Viviano  
Richard H. Bernstein  
Elizabeth T. Clement  
Megan K. Cavanagh

STATE OF MICHIGAN  
SUPREME COURT

PEOPLE OF THE STATE OF MICHIGAN,

Plaintiff-Appellee,

v

No. 158652

KRISTOPHER ALLEN HUGHES,

Defendant-Appellant.

---

VIVIANO, J. (*concurring*).

I concur in the majority’s holding but write separately because I take issue with one aspect of its reasoning. The majority identifies several factors that a court must consider to determine whether a police officer’s search of seized digital cell-phone data is reasonably directed at finding evidence of the criminal activity identified in the warrant. See *ante* at 26-30. I do not take issue with the factors identified by the majority, at least to the extent that they may apply in the cases to which they might be relevant.<sup>1</sup> But I believe the list is incomplete without the addition of another potentially dispositive factor: the officer’s subjective intention in conducting the search. If the search was purposefully conducted to obtain evidence of a crime other than the one identified in the warrant, I do not see how we can conclude that same search was “‘reasonably directed at uncovering’ evidence of the criminal activity alleged in the warrant.” *Ante* at 22.

---

<sup>1</sup> It is worth pointing out that, with the exception of Factor (h), the majority does not reference the factors or apply them in its analysis.

Citing conflicting caselaw from the federal circuit courts, the majority expressly declines to address whether the officer’s subjective intention is relevant to the inquiry. See note 13 of the majority opinion (comparing *United States v Loera*, 923 F3d 907 (CA 10, 2019), and *United States v Williams*, 592 F3d 511 (CA 4, 2010)). In *Loera*, the court persuasively explained why such a restriction is needed in the context of searches of electronic storage devices:

The general Fourth Amendment rule is that investigators executing a warrant can look anywhere where evidence described in the warrant might conceivably be located.

\* \* \*

This limitation works well in the physical-search context to ensure that searches pursuant to warrants remain narrowly tailored, but it is less effective in the electronic-search context where searches confront what one commentator has called the “needle-in-a-haystack” problem. Given the enormous amount of data that computers can store and the infinite places within a computer that electronic evidence might conceivably be located, the traditional rule risks allowing unlimited electronic searches.

To deal with this problem, rather than focusing our analysis of the reasonableness of an electronic search on “what” a particular warrant permitted the government agents to search (i.e., “a computer” or “a hard drive”), we have focused on “how” the agents carried out the search, that is, the reasonableness of the search method the government employed. Our electronic search precedents demonstrate a shift away from considering what digital location was searched and toward considering whether the forensic steps of the search process were reasonably directed at uncovering the evidence specified in the search warrant. Shifting our focus in this way is necessary in the electronic search context because search warrants typically contain few—if any—restrictions on where within a computer or other electronic storage device the government is permitted to search. Because it is “unrealistic to expect a warrant prospectively [to] restrict the scope of a search by directory, filename or extension or to attempt to structure search methods,” our [*ex post*] assessment of the propriety of a government search is essential to ensuring that the Fourth Amendment’s protections are realized

in this context. [*Loera*, 923 F3d at 916-917 (citations and emphasis omitted; first alteration in original).]

Later, in a footnote, the court acknowledged that inadvertence was abandoned as a necessary condition for a legitimate plain-view seizure in *Horton v California*, 496 US 128, 130, 139; 110 S Ct 2301; 110 L Ed 2d 112 (1990), but explained that it persisted in “includ[ing] inadvertence as a factor to consider when deciding whether an electronic search fell within the scope of its authorizing warrant or outside of it [because of] . . . [t]he fundamental differences between electronic searches and physical searches, including the fact that electronic search warrants are less likely prospectively to restrict the scope of the search . . . .” *Loera*, 923 F3d at 920 n 3.

A different approach was taken by the court in *Williams*, which was decided prior to *Riley v California*, 573 US 373; 134 S Ct 2473; 189 L Ed 2d 430 (2014). In that case, in examining the plain-view exception, the court held that a warrant authorizing a search of a computer and digital storage device “impliedly authorized officers to open each file on the computer and view its contents, at least cursorily, to determine whether the file fell within the scope of the warrant’s authorization . . . .” *Williams*, 592 F3d at 521. See also *id.* at 522 (“Once it is accepted that a computer search must, by implication, authorize at least a cursory review of each file on the computer, then the criteria for applying the plain-view exception are readily satisfied.”). Citing *Horton*, the court concluded that “[i]nadvertence focuses incorrectly on the subjective motivations of the officer in conducting the search and not on the objective determination of whether the search is authorized by the warrant or a valid exception to the warrant requirement.” *Id.* at 523. The court made it very clear that it would not adopt new rules to govern the search and seizure

of electronic files: “At bottom, we conclude that the sheer amount of information contained on a computer does not distinguish the authorized search of the computer from an analogous search of a file cabinet containing a large number of documents.” *Id.* at 523.

*Williams*’s approach is less persuasive in light of *Riley*. As the majority notes, “*Riley* distinguished cell-phone data from other items subject to a search incident to a lawful arrest in terms of the privacy interests at stake.” *Ante* at 15, citing *Riley*, 573 US at 393. In *Riley*, the government argued that a search of all data stored on a cell phone is “materially indistinguishable” from searches of other items found on an arrestee’s person. *Riley*, 573 US at 393. Apparently not impressed with this argument, the Court responded tartly: “That is like saying a ride on horseback is materially indistinguishable from a flight to the moon.” *Id.* The Court observed that “[o]ne of the most notable distinguishing features of modern cell phones is their immense storage capacity,” noting that “[t]he current top-selling smart phone has a standard capacity of 16 gigabytes . . . [which] translates to millions of pages of text, thousands of pictures, or hundreds of videos.” *Id.* at 393-394 (citation omitted). The rule adopted in *Loera*, which was decided after *Riley*, accounts for the realities of modern electronic storage devices. These privacy concerns are only heightened when it comes to the types and volume of data contained on modern smart phones, as the majority ably explains. See *ante* at 10-11, quoting *Riley*, 573 US at 393, 395-396.

Following the approach in *Loera*, I would adopt inadvertence as a factor to consider when deciding whether an electronic search fell within the scope of its authorizing warrant. Here, I would find that factor dispositive since it was clear that the second search of defendant’s cell phone was conducted to obtain evidence of a crime other than the drug-

trafficking offense identified in the warrant. At the time of the second search, the only crime defendant was charged with arising out of the August 6 incident was armed robbery. The prosecutor assigned to the armed-robbery case requested that the second search be conducted to obtain evidence to support that charge. Therefore, for this separate reason, I agree with the majority that the second search was beyond the scope of the warrant because it was not “reasonably directed at uncovering” evidence of drug trafficking.

Instead of relying on the lack of inadvertence, however, the majority focuses on whether there was any indication in the warrant or affidavit that that the searches performed would uncover evidence of defendant’s drug transactions with Weber or Stites. See *ante* at 31 (“There was nothing in the warrant or affidavit to suggest that either Weber or Stites was implicated in defendant’s drug trafficking or that reviewing data with Weber’s name or contacts with her phone number would lead to evidence regarding defendant’s drug trafficking.”); *ante* at 32 (“[A]ny connection between Weber and defendant’s drug trafficking was not derived from the warrant or its supportive affidavit.”). But I do not believe that a search warrant or the affidavit supporting it has to specify the participants of each drug transaction for that evidence to be within the scope of a drug-trafficking warrant.<sup>2</sup>

---

<sup>2</sup> See *United States v Castro*, 881 F3d 961, 966 (CA 6, 2018) (citation omitted) (“Officers may conduct a more detailed search of an electronic device after it was properly seized so long as the later search does not exceed the probable cause articulated in the original warrant and the device remained secured.”). If, for example, defendant had been charged with or was being investigated for a drug crime arising out of the August 6 incident, in my view, nothing would have precluded law enforcement officers from conducting a more detailed search of the properly seized cell-phone data using the new information they obtained concerning this additional instance of drug trafficking. See *id.* (“It is sometimes the case, as it was the case here, that law enforcement officers have good reason to revisit previously seized, and still secured, evidence as new information casts new light on the previously seized evidence.”). As the prosecutor points out, defendant’s interactions with

Such a requirement would go well beyond prospectively “considering whether the forensic steps of the search process were reasonably directed at uncovering the evidence specified in the search warrant.” *Loera*, 923 F3d at 917.<sup>3</sup>

Under the circumstances of this case, before conducting another search of defendant’s cell phone, the officer should have obtained a second search warrant directed toward obtaining evidence of the armed-robbery offense. Because he did not, I concur with the majority that the second search was unlawful under the Fourth Amendment.<sup>4</sup>

David F. Viviano

---

Weber and Stites on August 6 included the purchase and sale of illegal drugs. And once the evidence has been properly obtained, there is nothing that would prevent it from being used to prove a separate crime. See *Williams*, 592 F3d at 520, quoting *United States v Phillips*, 588 F3d 218, 224 (CA 4, 2009) (“ ‘Courts have never held that a search is overly broad merely because it results in additional criminal charges.’ ”). But we are not confronted with that situation. Instead, it is clear that the second search was conducted to obtain evidence of the alleged armed robbery.

<sup>3</sup> The majority’s reliance on this factor is perplexing for an additional reason: it is not one of the factors identified by the majority for determining whether a search is beyond the scope of the warrant. And I fear that it may lead to confusion about whether the absence of such details will constitute grounds to challenge the search and seizure of any drug-trafficking evidence that is not specifically referred to in the search warrant or affidavit.

<sup>4</sup> It appears that a plausible claim could be made that the government would have inevitably discovered the evidence contained on defendant’s cell phone through lawful means given that the cell phone was lawfully in the government’s possession. See *Loera*, 923 F3d at 928 (“When evidence is obtained in violation of the Fourth Amendment, that evidence need not be suppressed if agents inevitably would have discovered it through lawful means independent from the unconstitutional search.”). But since no such claim has been raised, I decline to consider it further.



Illinois (“ACLU of Illinois”) is the Illinois state affiliate of the national ACLU. Since its founding in 1920, the ACLU has frequently appeared before the Supreme Court and other state and federal courts in numerous cases implicating Americans’ right to privacy in the digital age, including as counsel in *Carpenter v. United States*, 138 S. Ct. 2206 (2018) and as *amicus* in *People v. Hughes*, No. 158652, 2020 WL 8022850 (Mich. Dec. 28, 2020), *United States v. Ganius*, 824 F.3d 199 (2d Cir. 2016), *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019), and *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). The ACLU of Illinois has appeared frequently before this Court advocating for the right to privacy and free speech in digital media and the right to privacy generally under the Fourth Amendment to the U.S. Constitution and Article 1, Section 6 of the Illinois Constitution. *Rosenbach v. Six Flags Entm't Corp.*, 2019 IL 123186; *People v. Morger*, 2019 IL 123643; *People v. Relerford*, 2017 IL 121094; *People v. Minnis*, 2016 IL 119563; *People v. Caballes*, 221 Ill. 2d 282 (2006); *King v. Ryan*, 153 Ill. 2d 449 (1992); *People v. Adams*, 149 Ill. 2d 331 (1992); *People v. Bartley*, 109 Ill. 2d 273 (1985); *People v. Cook*, 81 Ill. 2d 176 (1980).

2. *Amici* have unique experience advocating for strong privacy protections for personal information, including on the scope of search warrants for data on digital devices and the need for courts to give special scrutiny to, and impose concrete limitations on, warrants to search digital data.

**THIS AMICI BRIEF WILL ASSIST THE COURT**

3. This case involves the question of Americans’ privacy and possessory interests in intangible information, in a digital age where computers such as modern cell phones store for millions “the privacies of life,” *Riley*, 573 U.S. at 403 (quoting *Boyd v.*

*United States*, 116 U.S. 616, 630 (1886)). Indeed, today’s searches of computers and cell phones can expose to the government a “broad array” of records and sensitive information “never found in a home in any form,” *id.* at 396-97, making the need for courts to limit the scope of a digital search especially important.

4. The government’s arguments regarding the so-called “second look” doctrine and plain view doctrine in the context of digital device searches are of significant concern to *amici* as they threaten to establish a legal end run around the Fourth Amendment’s particularity and reasonableness requirements. *Amici* respectfully submit the proposed brief offering three reasons why the Appellate Court’s ruling should be upheld.

5. First, *amici* argue that individuals retain a privacy and possessory interest in their electronic data, regardless of whether such information is stored on an original hard drive or as, in Mr. McCavitt’s case, a mirrored EnCase replica. That the State duplicated Mr. McCavitt’s hard drive does not change, nor diminish those interests.

6. Second, the Peoria P.D.’s March 2014, post-acquittal search of McCavitt’s administratively overseized hard drive exceeded the authority granted by the July 2013 warrants, because it involved a search for evidence of different crimes committed against different victims. The State had no justification to retain the data, much less initiate another search for an entirely new investigation, at least not without first establishing probable cause and obtaining a warrant.

7. Third, the state’s arguments regarding the “second look” and plain view doctrines are inapposite in the context of warrant searches of administratively overseized devices. The state’s purported “second look” was temporally, purposively, and factually

distinct from the earlier searches for evidence pursuant to the warrants issued in July 2013. Further, the government searches do not meet the definition of “second looks.”

8. The plain view doctrine must also not be extended to the entire contents of a digital storage medium, like a hard drive, in which vast amounts of non-responsive information are intermingled with responsive evidence. As intentional overseizure without probable cause is part of the electronic search process, it requires “greater vigilance on the part of judicial officers in striking the right balance” to ensure that such overseizures do “not become a vehicle for the government to gain access to data which it has no probable cause to collect,” thereby making “every warrant for electronic information \*\*\*, in effect, a general warrant.” *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176-77 (9th Cir. 2010).

For these reasons, *amici* submit that the attached brief will be of service to the Court and respectfully request that this Court grant them leave to file the proposed brief of *amici curiae* in support of John T. McCavitt. A proposed order is attached to this Motion.

Dated: March 3, 2021

/s/ Rebecca K. Glenberg

Rebecca K. Glenberg  
ARDC No. 6322106  
Roger Baldwin Foundation of ACLU, Inc.  
150 N. Michigan Ave., Suite 600  
Chicago, IL 60601  
(312) 201-9740  
rglenberg@aclu-il.org

*On the Brief:*

Nusrat J. Choudhury  
Roger Baldwin Foundation of ACLU, Inc.  
150 N. Michigan Ave., Suite 600  
Chicago, IL 60601

Brett Max Kaufman  
Nathan Freed Wessler  
American Civil Liberties Union Foundation  
125 Broad Street  
New York, NY 10004

Jennifer Stisa Granick  
American Civil Liberties Union Foundation  
39 Drumm Street  
San Francisco, CA 94111

# Exhibit



*On the Brief:*

Nusrat J. Choudhury  
Roger Baldwin  
Foundation of ACLU, Inc.  
150 N. Michigan Ave., Suite 600  
Chicago, IL 60601

Brett Max Kaufman  
Nathan Freed Wessler  
American Civil Liberties  
Union Foundation  
125 Broad Street  
New York, NY 10004

Jennifer Stisa Granick  
American Civil Liberties  
Union Foundation  
39 Drumm Street  
San Francisco, CA 94111

**TABLE OF CONTENTS**

	<b>Page(s)</b>
<b>INTERESTS OF <i>AMICI CURIAE</i></b> .....	1
<b>FACTUAL BACKGROUND</b> .....	2
<b>SUMMARY OF ARGUMENT</b> .....	4

**POINTS AND AUTHORITIES**

<b>ARGUMENT</b> .....	6
<b>I. McCavitt maintained both privacy and possessory interests in copies of his hard drive</b> .....	6
U.S. Const., amend. IV .....	6
Ill. Const. 1970, art. 1, § 6 .....	6
<i>People v. LeFlore</i> , 2015 IL 116799.....	6
<i>People v. Caballes</i> , 221 Ill. 2d 282 (2006) .....	6
<i>People v. McDonough</i> , 239 Ill. 2d 260 (2010) .....	6
<i>Warden v. Hayden</i> , 387 U.S. 294 (1967).....	6
<i>Berger v. New York</i> , 388 U.S. 41 (1967).....	7
<i>Katz v. United States</i> , 389 U.S. 347 (1967).....	7
<i>People v. Smith</i> , 152 Ill. 2d 229 (1992) .....	7
<i>People v. Pitman</i> , 211 Ill. 2d 502 (2004) .....	7
<i>Riley v. California</i> , 573 U.S. 373 (2014).....	7, 8

<i>United States v. Jefferson</i> , 571 F. Supp. 2d 696 (E.D. Va. 2008) .....	7
Orin S. Kerr, <i>Fourth Amendment Seizures of Computer Data</i> , 119 Yale L.J. 700 (2010) .....	8
<i>Boyd v. United States</i> , 116 U.S. 616 (1886).....	8
<i>Arizona v. Gant</i> , 556 U.S. 332 (2009).....	8
<b>II. The March 2014 search was not a mere “second look” at previously viewed evidence</b> .....	8
<i>Brown v. Ohio</i> , 432 U.S. 161 (1977).....	9
<i>People v. Stefan</i> , 146 Ill. 2d 324 (1992) .....	9
<i>United States v. Edwards</i> , 415 U.S. 800 (1974).....	10, 11
<i>United States v. Burnette</i> , 698 F.2d 1038 (9th Cir. 1983) .....	10
<i>People v. Richards</i> , 94 Ill. 2d 92 (1983) .....	10
<i>United States v. Lackner</i> , 535 F. App’x 175 (3d Cir. 2013) .....	10
<i>Williams v. Commonwealth</i> , 527 S.E.2d 131 (Va. 2000) .....	10
<i>Hilley v. State</i> , 484 So. 2d 476 (Ala. Crim. App. 1985).....	10
<i>State v. Copridge</i> , 918 P.2d 1247 (Kan. 1996).....	10
<i>United States v. Jenkins</i> , 496 F.2d 57 (2d Cir. 1974) .....	10
<b>III. The March 2014 search of the EnCase copy exceeded the authority granted by the July 2013 warrants because it involved a search for evidence of different crimes committed against different victims</b> .....	11

<i>Maryland v. Garrison</i> , 480 U.S. 79 (1987).....	12
<i>Groh v. Ramirez</i> , 540 U.S. 551 (2004).....	12
<i>Illinois v. Gates</i> , 462 U.S. 213 (1983).....	12
<i>Katz v. United States</i> , 389 U.S. 347 (1967).....	12
<i>People v. Hughes</i> , No. 158652, 2020 WL 8022850 (Mich. Dec. 28, 2020).....	12
<i>United States v. Loera</i> , 923 F.3d 907 (10th Cir. 2019) .....	12
<i>Horton v. California</i> , 496 U.S. 128 (1990).....	12
<i>Gurleski v. United States</i> , 405 F.2d 253 (5th Cir. 1978) .....	13
<i>Riley v. California</i> , 573 U.S. 373 (2014).....	13
<i>United States v. Galpin</i> , 720 F.3d 436 (2d Cir. 2013) .....	13
<i>United States v. Comprehensive Drug Testing, Inc.</i> , 621 F.3d 1162 (9th Cir. 2010) .....	13
<i>United States v. Otero</i> , 563 F.3d 1127 (10th Cir. 2009) .....	13
<i>United States v. Carey</i> , 172 F.3d 1268 (10th Cir. 1999) .....	13
<i>Wheeler v. State</i> , 135 A.3d 282 (Del. 2016).....	13
<i>State v. Castagnola</i> , 145 Ohio St.3d 1, 2015-Ohio-1565, 46 N.E.3d 638 .....	14
<i>United States v. Walser</i> , 275 F.3d 981 (10th Cir. 2001) .....	14

<i>People v. Herrera</i> , 2015 CO 60.....	14
Orin S. Kerr, <i>Searches and Seizures in a Digital World</i> , 119 Harv. L. Rev. 531 (2005).....	14
<b>IV. The State unreasonably and unconstitutionally exploited its possession of overseized data that it had no justification to retain once McCavitt was acquitted.....</b>	<b>15</b>
<b>A. Overseizures of digital information are sometimes permitted for the limited purpose of facilitating warranted searches for responsive information, but courts must not permit the overseizure to enable law enforcement searches without probable cause.....</b>	<b>16</b>
<i>Riley v. California</i> , 573 U.S. 373 (2014).....	16, 18
<i>United States v. Comprehensive Drug Testing, Inc.</i> , 621 F.3d 1162 (9th Cir. 2010).....	16, 19
<i>United States v. Ganas</i> , 824 F.3d 199 (2d Cir. 2016) .....	16
<i>People v. Thompson</i> , 28 N.Y.S.3d 237 (Sup. Ct. 2016).....	16
<i>United States v. Premises Known as 608 Taylor Ave.</i> , 584 F.2d 1297 (3d Cir. 1978) .....	17
<i>People v. Hughes</i> , No. 158652, 2020 WL 8022850 (Mich. Dec. 28, 2020).....	17
<i>United States v. Matias</i> , 836 F.2d 744 (2d Cir. 1988) .....	17
<i>United States v. Veloz</i> , 109 F. Supp. 3d 305 (D. Mass. 2015).....	17
<i>In re Search of Information Associated with the Facebook Account Identified by the Username Aaron.Alexis that Is Stored at Premises Controlled by Facebook, Inc.</i> , 21 F. Supp. 3d 1 (D.D.C. 2013).....	17
<i>Andresen v. Maryland</i> , 427 U.S. 463 (1976).....	18

<i>United States v. Wey</i> , 256 F. Supp. 3d 355 (S.D.N.Y. 2017) .....	19
<i>In re Search Warrant</i> , 2012 VT 102, 193 Vt. 51, 71 A.3d 1158 .....	19
<i>United States v. Stetkiw</i> , No. 18-20579, 2019 WL 2866516 (E.D. Mich., July 3, 2019).....	19
<i>State v. Mansor</i> , 421 P.3d 323 (2018) .....	20
<b>B. The Court should not apply the plain view exception in this case.....</b>	<b>20</b>
<b>1. The plain view exception, developed for physical-world searches where evidence is tangible and discrete, is a poor fit for searches of digital information. ....</b>	<b>20</b>
<i>Arizona v. Gant</i> , 556 U.S. 332 (2009).....	21
<i>United States v. Jeffers</i> , 342 U.S. 48 (1951).....	21
<i>Collins v. Virginia</i> , 138 S. Ct. 1663 (2018).....	21
<i>City of Los Angeles v. Patel</i> , 576 U.S. 409 (2015).....	21
<i>Riley v. California</i> , 573 U.S. 373 (2014).....	21, 22
<i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018).....	21
<i>United States v. Cano</i> , 934 F.3d 1002 (9th Cir. 2019) .....	22
<i>United States v. Kolsuz</i> , 890 F.3d 133 (4th Cir. 2018) .....	22
<i>Horton v. California</i> , 496 U.S. 128 (1990).....	22
<i>United States v. Galpin</i> , 720 F.3d 436 (2d Cir. 2013) .....	22

<b>2. Reliance on the plain view doctrine to exploit an administrative overseizure is unreasonable in this case</b> .....	23
<i>Horton v. California</i> , 496 U.S. 128 (1990).....	23
<i>United States v. Galpin</i> , 720 F.3d 436 (2d Cir. 2013) .....	23
<i>People v. Hughes</i> , No. 158652, 2020 WL 8022850 (Mich. Dec. 28, 2020).....	23
<i>United States v. Gurczynski</i> , 76 M.J. 381 (C.A.A.F. 2017).....	24
<i>People v. Thompson</i> , 28 N.Y.S.3d 237 (Sup. Ct. 2016).....	24
<i>United States v. Wey</i> , 256 F. Supp. 3d 355 (S.D.N.Y. 2017) .....	24
<b>C. It was unreasonable for the State to re-search McCavitt’s data for evidence after his acquittal without obtaining a new warrant</b> .....	24
<i>Samson v. California</i> , 547 U.S. 843 (2006).....	25
<i>Riley v. California</i> , 573 U.S. 373 (2014).....	25, 26
<i>People v. Hughes</i> , No. 158652, 2020 WL 8022850 (Mich. Dec. 28, 2020).....	25
<b>CONCLUSION</b> .....	26

**INTERESTS OF AMICI CURIAE\***

The American Civil Liberties Union (“ACLU”) is a nationwide, nonprofit, nonpartisan organization dedicated to the principles of liberty and equality embodied in the Constitution and our nation’s civil rights laws. The American Civil Liberties Union of Illinois (“ACLU of Illinois”) is the Illinois state affiliate of the national ACLU.

Since its founding in 1920, the ACLU has frequently appeared before the Supreme Court and other state and federal courts in numerous cases implicating Americans’ right to privacy in the digital age, including as counsel in *Carpenter v. United States*, 138 S. Ct. 2206 (2018) and as *amicus* in *People v. Hughes*, No. 158652, 2020 WL 8022850 (Mich. Dec. 28, 2020), *United States v. Ganius*, 824 F.3d 199 (2d Cir. 2016), *United States v. Hasbajrami*, 945 F.3d 641 (2d Cir. 2019), and *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010). The ACLU of Illinois has appeared frequently before this Court advocating for the right to privacy and free speech in digital media and the right to privacy generally under the Fourth Amendment to the U.S. Constitution and Article 1, Section 6 of the Illinois Constitution. *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186; *People v. Morger*, 2019 IL 123643; *People v. Relerford*, 2017 IL 121094; *People v. Minnis*, 2016 IL 119563; *People v. Caballes*, 221 Ill. 2d 282 (2006); *King v. Ryan*, 153 Ill. 2d 449 (1992); *People v. Adams*, 149 Ill. 2d 331 (1992); *People v. Bartley*, 109 Ill. 2d 273 (1985); *People v. Cook*, 81 Ill. 2d 176 (1980).

---

\* *Amici* wish to thank Eli Hadley and Santana V. Jackson, students in the Technology Law & Policy Clinic at New York University School of Law, for their contributions to this brief.

## FACTUAL BACKGROUND

On July 17, 2013, the Illinois State Police (I.S.P.) obtained a warrant authorizing a search of John T. McCavitt’s home and seizure of computers found there. Approximately a week later, on July 24, the I.S.P. obtained a second warrant to search the data stored on a cellphone as well as a LG computer tower. A19-20; A29<sup>1</sup> (together, the “July 2013 warrants”). That second warrant authorized a search for any digital images, stored or deleted data, or other evidence of the crimes of aggravated criminal sexual assault, unlawful restraint, and unauthorized video recording/live video transmission. The affidavit in support of that search warrant alleged that these crimes were committed against a specific and named victim in a single incident that took place the early morning of July 17, 2013. A25-26. There were no allegations to support probable cause for any other crime.

A forensic examiner for the Peoria County Sheriff’s Department (“Peoria C.S.D.”), Jeff Avery, worked with the I.S.P. to conduct a forensic examination of the LG computer tower. The examiner used EnCase forensic software to create “a bit-by-bit image” reflecting all data on McCavitt’s hard drive (hereafter the “EnCase copy”). Tr. Mot. Suppress Evid., R17, 23-24. The examiner then performed the forensic exam. R24-25. Subsequently, in August of 2013, the State charged McCavitt with two sexual-assault-related offenses, to which McCavitt pleaded not guilty. Op. of Ill. App. Ct., Third Dist., A2, ¶ 5. The case proceeded to trial and, on March 19, 2014, a jury found McCavitt not guilty of all charges. *Id.* On that same day, McCavitt orally requested the return of his

---

<sup>1</sup> Citations to “A\_” refer to the Appendix to the Brief of Plaintiff-Appellant People of the State of Illinois (hereinafter “Pl. App. Br.”), filed 10/13/20. Citations to “R\_” refer to the report of proceedings.

personal property, including his computer. The court denied the request, stating that the property would be returned to him when everything “cooled down.” *Id.*

On March 20, 2014, just one day after McCavitt’s acquittal, the Peoria Police Department (“Peoria P.D.”) initiated an “internal” investigation into McCavitt, an officer at the department. A2, ¶ 6; R30. The following day, the Peoria P.D. forensic examiner, James Feehan, requested and received the EnCase copy from Peoria C.S.D. examiner Avery. *Id.* On March 24, Peoria P.D.’s Feehan began a digital forensic analysis of the EnCase copy, without a warrant (the “March 2014 search”), and saw two images of what he believed to be child pornography. A2, ¶ 6. More than a week later, on April 1, the Peoria P.D. sought and obtained a warrant to further search McCavitt’s EnCase copy for images of child pornography. A2, ¶ 7; R34. On April 28, the State indicted McCavitt based on images found in his EnCase copy. A2, ¶ 7. McCavitt filed a motion to suppress the child pornography evidence obtained from the EnCase copy, arguing that the Peoria P.D. had no authority to warrantlessly obtain or examine his hard drive data in March 2014. *Id.*, ¶ 8.

At the suppression hearing, Peoria P.D. examiner Feehan testified that—despite being aware of McCavitt’s March acquittal—he had requested the EnCase copy of McCavitt’s hard drive, believing “in the back of [his] mind that there was [*sic*] other victims that could be identified.” R29-30, R32, R38. He also testified that he “knew,” at the time, that Peoria P.D.’s internal investigation “would parallel” a criminal investigation, because “[d]epending on the outcome of the internal [investigation], \*\*\* it could possibly be criminal, as [wa]s with most cases [the Peoria P.D.] deal[t] with in circumstances like this.” R40-41. Peoria P.D.’s Feehan also testified that he sought and

obtained the April 1 search warrant for two reasons: (1) it would be “safe[r]” to get a warrant “specifically for child pornography,” as the prior warrant permitted only searches for evidence of criminal sexual assault and (2) following McCavitt’s March 28 arrest, the investigation had shifted from a formal internal investigation to a criminal investigation.

R35; Pl. App. Br. 6.

The trial court denied McCavitt’s motion to suppress, and, in 2016, a jury convicted him of possession of child pornography. R667-69.

On appeal, the Third District Appellate Court of Illinois reversed the trial court’s denial of the motion to suppress, holding that Peoria P.D.’s warrantless search of McCavitt’s computer hard drive data following his acquittal on previous unrelated charges violated McCavitt’s right to privacy under the Fourth Amendment to the United States Constitution. A1-5. The appellate court held that McCavitt had a diminished expectation of privacy in his seized computer files until his trial was complete. But after that, McCavitt could again expect that he had a full right to privacy in those files. A4, ¶ 24. When Feehan searched McCavitt’s EnCase copy without a warrant in March 2014, the search violated that full expectation of privacy. *Id.* ¶ 25. The court also rejected the State’s invocation of the good-faith exception to the exclusionary rule, finding that Feehan did not act in good faith in concluding that he could perform a warrantless search of the EnCase copy after McCavitt’s acquittal. *Id.* ¶ 31.

### **SUMMARY OF ARGUMENT**

First, under both the Fourth Amendment and Article I, Section 6 of the Illinois Constitution, McCavitt maintained constitutional privacy and possessory interests in the copies of the data on his hard drive—and not just the hard drive itself—that were

searched by law enforcement. As a result, any search of that data presumptively requires a valid warrant.

Second, the State is wrong to insist that its warrantless searches of McCavitt's data are excused by the "second look" doctrine. The March 2014 search at issue here was temporally, purposively, and factually distinct from the earlier searches for evidence pursuant to the July 2013 warrants. In any event, the "second look" doctrine has no application in the context of searches pursuant to warrants, but merely applies to searches of physical items seized incident to arrest and inventoried in police stations. And even if the doctrine did apply here, any "second look" was constitutionally unreasonable under the totality of the circumstances.

Third, the March 2014 search at issue here involved a search for evidence of different crimes committed against different victims than the one authorized by two warrants in July 2013, and the authority of those earlier warrants did not reach the State's post-acquittal searches of McCavitt's data.

Fourth, the State's exploitation of its ongoing possession of a copy of McCavitt's data was constitutionally unreasonable for several reasons. While overseizures of data are often permissible in the context of seizures and searches of digital information, those overseizures are explicitly allowed for the limited purpose of enabling law enforcement to conduct a warranted search based on probable cause. To permit law enforcement to exploit such overseizures beyond the scope of a valid warrant risks permitting any search of digital information to expand into the type of "general search" reviled by the Founders. Moreover, the plain view doctrine does not excuse the State's warrantless search here. The doctrine, which developed in cases involving physical limitations that cabined its

reach, is a poor fit for the digital realm. And to permit the State to overseize data for one purpose but claim the benefit of “plain view” months later would be unreasonable.

Finally, that the State engaged in its new searches after McCavitt’s acquittal of the crimes under investigation, and for which the original warrants issued, is likewise unreasonable.

## ARGUMENT

### **I. McCavitt maintained both privacy and possessory interests in copies of his hard drive.**

Today’s computer hard drives store huge volumes of digital data. “Mirroring” software (here, EnCase) creates a perfect replica of the data on a hard drive. R17, 22-23, 46. An individual has the same privacy and possessory interests in their electronic data regardless of whether it is stored on the original hard drive or is a copy of that data, and the State’s contrary argument is incorrect.

The Fourth Amendment to the United States Constitution and Article 1, Section 6 of the Illinois Constitution prohibit unreasonable searches and seizures. U.S. Const., amend. IV; Ill. Const. 1970, art. 1, § 6. This Court “interprets the search and seizure clause of the Illinois Constitution in ‘limited lockstep’ with its federal counterpart.” *People v. LeFlore*, 2015 IL 116799, ¶ 16 (quoting *People v. Caballes*, 221 Ill. 2d 282, 314 (2006)). “The essential purpose of the fourth amendment is to impose a standard of reasonableness upon the exercise of discretion by law enforcement officers to safeguard the privacy and security of individuals against arbitrary invasions” (quotation marks omitted). *People v. McDonough*, 239 Ill. 2d 260, 266 (2010).

The Fourth Amendment protects one’s reasonable expectation of privacy in intangible material as well as tangible items. *See Warden v. Hayden*, 387 U.S. 294, 304

(1967) (Fourth Amendment protects privacy independent from property concepts). For example, the Fourth Amendment prohibits government eavesdropping on private conversations without a valid warrant. *Berger v. New York*, 388 U.S. 41, 51 (1967) (conversations); *Katz v. United States*, 389 U.S. 347, 353 (1967) (same). The Illinois Constitution similarly offers “protect[ion] [to] people, not places.” *People v. Smith*, 152 Ill. 2d 229, 244 (1992) (citing *Katz*, 389 U.S. at 351); see *People v. Pitman*, 211 Ill. 2d 502, 514 (2004).

The constitutional privacy interest in intangibles applies to copies like the EnCase copy. In *Riley v. California*, the Supreme Court permitted police to seize a cell phone without a warrant pursuant to the search-incident-to-arrest doctrine, but barred them from searching the information contained in the phone without further justification. 573 U.S. 373, 403 (2014). In so holding, the Court recognized that the defendant’s privacy and possessory interests in the data stored in a phone were separate from—and more extensive than—his interests in the physical phone itself. *Id.* at 393. Moreover, the fact that the police had physical possession of the phone did not diminish the defendant’s expectation of privacy in the information stored on the device. Accordingly, the Fourth Amendment’s protection “extends not just to the paper on which the information is written or the disc on which it is recorded but also to the information on the paper or disc itself.” *United States v. Jefferson*, 571 F. Supp. 2d 696, 702 (E.D. Va. 2008) (holding that taking high-resolution photographs of documents and taking notes on the contents of documents constituted a search and seizure of the information contained in those documents).

Likewise, in this case, McCavitt's privacy interests in the *information* that was stored in his computer at the time it was seized exists separately from his interests in the physical hard drive itself. That the State duplicated that information in the form of the EnCase copy does not change or diminish those interests. *See, e.g.,* Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 Yale L.J. 700, 703 (2010) (explaining that an individual's "possessory interest extends to both the original and any copies made from it" and that the owner's possessory interest is in "the data"); *see also infra* Part IV.A (explaining the limited purpose of "administrative overseizure" in connection with the seizure and search of information on digital devices).

In the digital age, the Fourth Amendment's protection of privacy and possessory interests in intangible information is more important than ever. Computers, like modern cell phones, hold for many Americans "the privacies of life." *Riley*, 573 U.S. at 403 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)). Searches of computers, including modern cell phones, would typically expose to the government far more than the most exhaustive search of a house: "A [digital device] not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form." *Id.* at 396-97.

Because McCavitt retained a possessory interest and expectation of privacy in the EnCase copy of his hard drive, any search of that data presumptively requires a valid warrant. *Arizona v. Gant*, 556 U.S. 332, 344 (2009). As explained below, no such warrant authorized the March 2014 search conducted by the Peoria P.D.

**II. The March 2014 search was not a mere "second look" at previously viewed evidence.**

The State represents that its March 2014 search of McCavitt's hard drive was simply a harmless "second look" at the same evidence viewed under the first warrant. Pl. App. Br. 12. This is incorrect.

First, the March 2014 search was temporally, purposively, and factually distinct from the earlier searches for evidence pursuant to the July 2013 warrants. The search was conducted by a different law enforcement agency (the Peoria P.D.) than the one that had conducted the original searches (the Peoria C.S.D.). R17-19. Moreover, the search was explicitly conducted for a new investigative purpose. Indeed, Detective Feehan testified that he was conducting the Peoria P.D. search for an "internal affairs investigation" as well as for evidence of crimes not yet discovered. R30, 32. The March 2014 search sought to uncover never-before-seen evidence of offenses committed against different victims, at different times, and not the single victim and single crime covered by the July 2013 warrants. *Compare* R32 with A16-18 and 25-28. Further, as the appellate court emphasized, A5, ¶¶ 30-31, the March 2014 search took place the day after a months-long investigation had ended in McCavitt's acquittal. Surely, the State's decision to take McCavitt's case to trial and receive a jury verdict indicated that the I.S.P. and the prosecution had exhausted their criminal investigation, and any subsequent searches of the hard drive were, by definition, in support of a new one.<sup>2</sup>

Second, the "second look" doctrine does not extend to searches conducted pursuant to warrants. As the State concedes, Pl. App. Br. 12-13, this doctrine applies to

---

<sup>2</sup> The Peoria P.D.'s search would have been entirely pointless had it been intended to simply re-execute prior searches, as the State cannot try McCavitt a second time for the same crimes. *See Brown v. Ohio*, 432 U.S. 161, 165 (1977) (Double Jeopardy Clause "protects against a second prosecution for the same offense after acquittal"); *People v. Stefan*, 146 Ill. 2d 324, 333 (1992) (same).

searches of physical items seized incident to arrest and inventoried in police stations. *See, e.g., United States v. Edwards*, 415 U.S. 800 (1974) (reexamination of a defendant’s clothes); *United States v. Burnette*, 698 F.2d 1038 (9th Cir. 1983) (reexamination of a purse); *People v. Richards*, 94 Ill. 2d 92 (1983) (reexamination of a necklace). The State cites no case with a fact pattern remotely similar to this one. Rather, it argues that the “second look” doctrine applies “seamless[ly]” to this case because searches incident to arrest and warranted searches both require probable cause. Pl. App. Br. 13. It represents that *Burnette* “expanded” the logic of *Edwards* “to apply beyond its factual context.” *Id.* at 13. But *Burnette*, too, involved a search incident to arrest. *See* 698 F.2d at 1049.<sup>3</sup> The “second look” doctrine is irrelevant in the context of warranted searches because the warrant itself and the Fourth Amendment rules around the execution of that warrant govern the legality of the search. *See infra* Part IV.C.

Third, even if the doctrine applies in this context, “second looks” must be confined to evidence “previously seen” by the government, and cannot be extended to “discover[ies of] new evidence.” *Richards*, 94 Ill. 2d at 99; *United States v. Jenkins*, 496 F.2d 57, 74 (2d Cir. 1974) (second look invaded no reasonable expectations of privacy when the police officers “simply looked again at what they had already— lawfully— seen”). Here, the evidence McCavitt sought to suppress was never seen by the

---

<sup>3</sup> The State also cites *United States v. Lackner*, 535 F. App’x 175, 180-181 (3d Cir. 2013) (FBI agents could participate in search pursuant to warrant), *Williams v. Commonwealth*, 527 S.E.2d 131, 136 (Va. 2000) (search of property administratively seized from arrestee), *Hilley v. State*, 484 So. 2d 476, 481 (Ala. Crim. App. 1985) (purse lawfully seized incident to arrest and subject to inventory searches), and *State v. Copridge*, 918 P.2d 1247, 1251-52 (Kan. 1996) (search of property conducted while defendant was being booked into jail). None of these cases come close to supporting the State’s argument.

government prior to the March 2014 search. It was obtained via a search for information about victims other than the victim named in the July 2013 warrants. Indeed, as explained *infra* Part IV.B, this information was in government hands in March 2014 only because it knowingly *overseized* McCavitt's entire hard drive as a matter of administrative convenience, rather than seizing only the responsive portions of the drive.

Finally, as the Supreme Court explained in *Edwards*, "second looks" are permitted only for "a reasonable time and to a reasonable extent," 415 U.S. at 809. In other words, they are subject to Fourth Amendment reasonableness, as any search must be. As explained below, it was not reasonable for the government to continue to search McCavitt's private information once he was acquitted. As the Appellate Court wrote, "no reasonably trained officer would conclude that he could perform a warrantless search of a mirrored hard drive that he had no right to possess following the termination of the criminal case against defendant." A5, ¶ 31.

**III. The March 2014 search of the EnCase copy exceeded the authority granted by the July 2013 warrants because it involved a search for evidence of different crimes committed against different victims.**

The Peoria P.D.'s post-acquittal search was not authorized by the July 2013 warrants. Those warrants permitted a different law enforcement agency to search for evidence of three specified crimes against a single named individual allegedly occurring on July 17, 2013. Neither the July 2013 warrants nor the affidavits supporting them pertained to information from other dates or images of other people. Under the Fourth Amendment, all searches must be within the scope of the warrant authorizing them (and justifying their invasion of a person's reasonable expectation of privacy), and warrants

may not authorize fishing expeditions for evidence of offenses for which there is no probable cause.

A warrant establishes the boundaries of a lawful search. The Fourth Amendment’s particularity requirement “ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the [Fourth Amendment was] intendeds to prohibit.” *Maryland v. Garrison*, 480 U.S. 79, 84 (1987); *see also Groh v. Ramirez*, 540 U.S. 551, 557 (2004) (emphasizing that warrants must provide a specific description of the evidence sought). The warrant must be specific enough to ensure that the judge, not the officer, fixes the scope of the search. *Illinois v. Gates*, 462 U.S. 213, 240 (1983).

That scope is limited by the probable cause, demonstrated in a warrant affidavit, to believe that searching a particular place will lead to evidence of a particular crime. Critically, this means that warrants authorize the government to invade privacy interests only with respect to information that is responsive to a valid warrant. Searches for evidence of *other* offenses not described in the warrant are unconstitutional because they are warrantless—and warrantless searches are *per se* unreasonable unless they fall into an exception. *See Katz*, 389 U.S. 347. As the Michigan Supreme Court recently explained:

[A]s with any other search conducted pursuant to a warrant, a search of digital data from a cell phone must be “reasonably directed at uncovering” evidence of the criminal activity alleged in the warrant and that any search that is not so directed but is directed instead toward finding evidence of other and unrelated criminal activity is beyond the scope of the warrant.

*People v. Hughes*, No. 158652, 2020 WL 8022850, at \*13 (Mich. Dec. 28, 2020) (quoting *United States v. Loera*, 923 F.3d 907, 917, 922 (10th Cir. 2019), and citing *Horton v. California*, 496 U.S. 128, 140-41 (1990)); *see also Gurlleski v. United States*,

405 F.2d 253, 258 (5th Cir. 1978) (“[T]he search must be one directed in good faith toward the objects specified in the warrant or for other means and instrumentalities by which the crime charged had been committed.”).

In recent years, courts have become especially attuned to the need for strict application of the traditional Fourth Amendment guardrails, like the particularity requirement, to search warrants for digital information. The particularity requirement is especially important in the digital context, where there are few practical barriers to law enforcement’s expanding the scope of a search, unless magistrates and the government take careful precautions. As the Supreme Court explained in *Riley*, there are “substantial privacy interests \*\*\* at stake when digital data is involved.” 573 U.S. at 375. These heightened interests require courts to vigilantly protect the proper bounds of digital searches. *See, e.g., United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013) (discussing the need for “heightened sensitivity to the particularity requirement in the context of digital searches” due to the vast amount of information that digital devices contain); *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (discussing the “serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant”); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) (ability of a computer to store “a huge array” of information “makes the particularity requirement that much more important”); *United States v. Carey*, 172 F.3d 1268, 1275 n.7 (10th Cir. 1999) (discussing the court’s “belief that the storage capacity of computers requires a special approach” to particularity and the execution of searches of digital media); *Wheeler v. State*, 135 A.3d 282, 307 (Del. 2016) (risk for warrants for digital and electronic devices to become “general warrants” is

substantial, which “necessitates heightened vigilance, at the outset, on the part of judicial officers to guard against unjustified invasions of privacy”); *State v. Castagnola*, 145 Ohio St.3d 1, 2015-Ohio-1565, ¶¶ 77-78, 46 N.E.3d 638, (due to the large amount of information on computers, officers must be clear about what they are “seeking on the computer and conduct the search in a way that avoids searching files of types not identified in the *warrant*”) (emphasis added and citing *United States v. Walser*, 275 F.3d 981, 986 (10th Cir. 2001); *People v. Herrera*, 2015 CO 60, ¶ 18 (in executing a search warrant for evidence related to a suspected crime involving a particular victim, it violates the Fourth Amendment for law enforcement officers to open a file labeled with the name of a different possible victim even where the suspected crime was the same); *see also* Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 565 (2005) (explaining that without careful attention to particularity, “today’s diminished protections are likely to shrink even more as technology advances”).

Here, the March 2014 search went beyond scope of the July 2013 warrants, which permitted searches for evidence of criminal sexual assault, unlawful restraint, and unauthorized video recording of a single, named victim stemming from a single incident on July 17, 2013. A16, 19, 21, 27.<sup>4</sup> But the Peoria P.D.’s examiner testified that in March 2014, he went back to search McCavitt’s EnCase copy to find evidence related to other, unnamed victims, evidence for which the State had not established probable cause supporting a warrant. *See* Pl. App. Br. 24 (“[Peoria P.D.’s] Feehan explained that he ‘knew that there were other victims that could be identified’ that could lead to future

---

<sup>4</sup> The second July 2013 warrant mentioned a video of an unidentified person, but did not provide any reason to believe that that video was surreptitiously taken or that that person was an additional victim. A27.

criminal charges.”); R32 (“[I]n the back of my mind, I knew that there was [*sic*] other victims that could be identified during the formal [internal affairs investigation] that would turn criminal.”); R38 (discussing “the possibility of identifying the other victims during our internal investigation, that possibility existed and then could ultimately come back to State's Attorney’s Office for review and possible charges”). This search was conducted for purposes of both criminal and internal affairs investigation. It impermissibly included searches for images that were taken on dates other than July 17.

Because a law enforcement agent intentionally searched for evidence of a crime that was not under investigation and not detailed in the affidavits in support of the July 2013 warrants and thus for which there was no probable cause, the search was warrantless and unconstitutional.

**IV. The State unreasonably and unconstitutionally exploited its possession of overseized data that it had no justification to retain once McCavitt was acquitted.**

The appellate court correctly held that, once McCavitt was acquitted, the State had no valid interest in retaining the EnCase copy. The State contends that because the Illinois State Police obtained a valid warrant as part of its investigation into McCavitt for a specific incident of aggravated criminal sexual assault, it was permitted to search McCavitt’s hard drive months later—even after he was acquitted of the crimes the warrant was intended to investigate. But as explained below, the State only possessed the later-discovered evidence because it had been permitted to seize (and copy) McCavitt’s entire drive for a purely administrative purpose—to enable it to search for data that *was* covered by (and justified by the probable cause shown in) the July 2013 warrants. Law enforcement cannot facilitate additional invasions of privacy through this kind of bait and

switch, and neither the plain view doctrine nor the fact of the initial overseizure justified the later search.

**A. Overseizures of digital information are sometimes permitted for the limited purpose of facilitating warranted searches for responsive information, but courts must not permit the overseizure to enable law enforcement searches without probable cause.**

Searches of digital devices often include the intentional overseizure of information, without probable cause, for law enforcement's administrative convenience. Courts must therefore ensure that searches of this overseized data are strictly limited by probable cause, particularity, and the terms of the warrant lest they become unconstitutional general searches.

Given the vast amount of information housed on digital devices, *Riley*, 573 U.S. at 386, the entire contents of a digital storage medium, like a hard drive, will almost never be responsive to a validly drawn warrant. *Comprehensive Drug Testing*, 621 F.3d at 1168-70 (in the digital context, responsive information will almost always be intermingled with nonresponsive information). However, it is generally challenging for law enforcement to conduct searches of a digital device for responsive information at the scene of that device's seizure. To facilitate forensically sound law enforcement searches of digital data, then, modern warrants regularly permit device seizures, knowing that this will result in an *overseizure* of information, placing into the government's possession information that it has no justification to search. The basis for this practice is that it permits law enforcement to locate and secure responsive information covered by the warrant. *See United States v. Ganius*, 824 F.3d 199, 216 (2d Cir. 2016); *see also, e.g., People v. Thompson*, 28 N.Y.S.3d 237, 258 (Sup. Ct. 2016) ("The Defendant's non-

responsive emails were never properly seized by the People. They were provided as an administrative convenience to allow an effective search.”).

Such overseizures are a practical solution to a specific problem, but that solution raises the question of how law enforcement handles, preserves, and uses non-responsive information on seized digital devices. If the government is permitted to seize materials beyond the scope of a properly narrow warrant, but then later exploit the overseizure anytime it wishes—as it did in this case—it undermines the particularity requirement so essential to ensuring that searches and seizures are constitutional. As the appellate court in this case put it, “While police lawfully created the EnCase file to forensically examine defendant’s hard drive, they were not entitled to retain the entire EnCase file indefinitely.” A4, ¶ 25 (citing *United States v. Premises Known as 608 Taylor Ave.*, 584 F.2d 1297, 1302 (3d Cir. 1978)). That is because permission to search for responsive material connected to probable cause *does not* extend to non-responsive data, information in which an individual maintains a full expectation of privacy. *See, e.g., Hughes*, 2020 WL 8022850, at \*9 (“The question here is whether the seizure and search of cell-phone data pursuant to a warrant extinguishes that otherwise reasonable expectation of privacy in the entirety of that seized data. We conclude that it does not. Rather, a warrant authorizing the police to seize and search cell-phone data allows officers to examine the seized data only to the extent reasonably consistent with the scope of the warrant.”); *see also* A4, ¶ 25 (citing *United States v. Matias*, 836 F.2d 744, 747 (2d Cir. 1988); *United States v. Veloz*, 109 F. Supp. 3d 305, 313 (D. Mass. 2015); *In re Search of Information Associated with the Facebook Account Identified by the Username Aaron.Alexis that Is*

*Stored at Premises Controlled by Facebook, Inc.*, 21 F. Supp. 3d 1, 10 (D.D.C. 2013); *Thompson*, 28 N.Y.S.3d at 258-59) .

In *Andresen v. Maryland*, the Supreme Court recognized that there are “grave dangers inherent in executing a warrant authorizing a search and seizure of a person’s papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable.” 427 U.S. 463, 482 n.11 (1976). These dangers are amplified when a warrant addresses digital information, where a search will implicate not only great volumes of “papers,” but an unprecedented diversity of other private information as well. *See Riley*, 573 U.S. at 394 (“[A] cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. [And] a cell phone’s capacity allows even just one type of information to convey far more than previously possible.”). Critically, the Supreme Court in *Andresen* observed that the “State was correct in returning [papers that were not within the scope of the warrants or were otherwise improperly seized] voluntarily [to the owner],” and that the “trial judge was correct in suppressing others.” 427 U.S. at 482 n.11. The Court cautioned that, when faced with searches and seizures of this scope, “responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.” *Id.*

Indeed, courts have grown increasingly concerned about unreasonable privacy invasions stemming from careless or opportunistic searches of intermingled digital data. For example, in *Comprehensive Drug Testing Inc.*, the Ninth Circuit explained that administrative overseizure creates a serious risk “that every warrant for electronic

information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant.” 621 F.3d at 1176. Because overseizure is part of the electronic search process, it requires “greater vigilance on the part of judicial officers in striking the right balance” to ensure that overseizures do “not become a vehicle for the government to gain access to data which it has no probable cause to collect.” *Id.* at 1177; *see also United States v. Wey*, 256 F. Supp. 3d 355, 407 (S.D.N.Y. 2017) (likening a warrantless search of overseized, non-responsive digital information to “the Government seizing some hard-copy notebooks while leaving others it deemed unresponsive behind, and then returning to the premises two years later to seize the left-behind notebooks based on investigative developments but without seeking a new warrant”); *Thompson*, 28 N.Y.S. 3d at 259 (administrative convenience is not “license for the government to retain tens of thousands of a defendant’s non-relevant personal communications to review and study at their leisure”). Other courts have followed that lead, suggesting that flexible *ex ante* protocols be set out by magistrates on a case by case basis to prevent law enforcement from unnecessarily viewing non-responsive files during the execution of a search warrant in the digital context. *In re Search Warrant*, 2012 VT 102, 193 Vt. 51, 71 A.3d 1158 (upholding nine restrictions on a search warrant for electronic data); *United States v. Stetkiw*, No. 18-20579, 2019 WL 2866516 (E.D. Mich., July 3, 2019). As the Supreme Court of Oregon, under its state analogue to the Fourth Amendment, recently explained:

We acknowledge that, for practical reasons, searches of computers are often comprehensive and therefore are likely to uncover information that goes beyond the probable cause basis for the warrant. In light of that fact, to protect the right to privacy and to avoid permitting the digital equivalent of general warrants, we also hold that Article I, section 9, prevents the state from using evidence found in a computer search unless a valid warrant authorized the search for that particular evidence, or it is

admissible under an exception to the warrant requirement. *State v. Mansor*, 421 P.3d 323, 326 (2018).

Like these courts, this Court should reinforce the importance of exacting and scrupulous application of Fourth Amendment principles to searches of digital information. It is quickly becoming the norm for the government to seize extraordinary amounts of digital data in the pursuit of a narrow slice of information. The government is poised, in other words, to create ever larger stockpiles of information to be searched later, if and when it determines a need—as it did in this case. The result would be a return to the very sort of activity that the Fourth Amendment’s drafters meant to combat: the government’s indiscriminate and warrantless collection of private information. Instead, this Court should hold that it is unreasonable to retain and search information for which there is no probable cause, and which could have been returned and/or deleted from law enforcement databases or other data storage devices.

**B. The Court should not apply the plain view exception in this case.**

The Court should reject the State’s argument that the plain view doctrine somehow permits law enforcement agencies to engage in new searches of overseized data. The plain view exception to the warrant requirement should not be extended to searches of voluminous digital data, but even to the extent the doctrine might sometimes apply, it cannot justify the search at issue here.

**1. The plain view exception, developed for physical-world searches where evidence is tangible and discrete, is a poor fit for searches of digital information.**

Exceptions to the warrant requirement, such as the plain view doctrine, do not apply automatically upon invocation; rather, they must remain “tether[ed]” to “the

justifications underlying the \*\*\* exception.” *Gant*, 556 U.S. at 343. The government bears the burden of demonstrating that an exception to the warrant requirement ought to apply in a given context. *United States v. Jeffers*, 342 U.S. 48, 51 (1951). Time and again, the Supreme Court has refused to “unmoor [warrant] exception[s] from [their] justifications \*\*\* and transform what was meant to be an exception into a tool with far broader application.” *Collins v. Virginia*, 138 S. Ct. 1663, 1667, 1672-73 (2018).<sup>5</sup>

The Supreme Court has been particularly skeptical of the application of analogue-era exceptions to new digital contexts. *See, e.g., Riley*, 573 U.S. at 393; *see also Carpenter v. United States*, 138 S. Ct. 2206, 2222 (2018) (explaining that pre-digital Fourth Amendment precedents cannot be mechanically extended to cases involving digital-age searches). In *Riley*, the Court declined to extend the search-incident-to-arrest exception developed in cases involving arrestees’ possession of items like cigarette packs to the digital information contained on an arrestee’s cell phone. There, the government “assert[ed] that a search of all data stored on a cell phone [was] ‘materially indistinguishable’ from searches of \*\*\* physical items,” but the Court issued a harsh rejoinder:

---

<sup>5</sup> For example, in *Gant*, the Court declined to extend the search-incident-to-arrest exception to the warrantless search of a passenger compartment in defendant-arrestee’s vehicle where it was “unnecessary to protect law enforcement safety and evidentiary interests.” 556 U.S. at 346. In *Collins v. Virginia*, the Court held that the automobile exception does not allow an officer to enter a home or its curtilage without a warrant because, unlike vehicles, the curtilage of a home is not readily mobile. 138 S. Ct. at 1672-73. And in *City of Los Angeles v. Patel*, the Court declined to apply the exception for closely regulated industries to warrantless searches of hotel guest registries because, unlike inherently dangerous industries with a history of government oversight such that no proprietor could have a reasonable expectation of privacy, “nothing inherent in the operation of hotels poses a clear and significant risk to the public welfare.” 576 U.S. 409, 424 (2015).

That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee's pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom. 573 U.S. at 393.

Holding otherwise would have “untether[ed] the rule from the justifications underlying the [search-incident-to-arrest] exception”—that is, officer safety and evidence preservation. *Id.* at 386.

For similar reasons, the Fourth and Ninth Circuits have recently rejected the government's argument that the “border search exception,” which is justified by the government's interest in interdicting physical contraband, could be expanded to permit invasive, suspicionless searches of travelers' electronic devices conducted at a national border. *United States v. Cano*, 934 F.3d 1002 (9th Cir. 2019); *United States v. Kolsuz*, 890 F.3d 133, 138 (4th Cir. 2018).

As with these limited exceptions to the warrant requirement, the underlying justifications for the plain view doctrine do not translate to the digital context. In the physical world, the benefits to law enforcement from the plain view exception are limited by the physical characteristics of the things and places for which there is probable cause to search. For example, warrants may easily restrict a physical search to those places large enough to hold the items particularly described in the warrant. Even where police are lawfully in a home, they cannot benefit from plain view by opening a spice box when searching for a rifle. *See, e.g., Horton*, 496 U.S. at 141. Nor can they do so by rummaging through a medicine cabinet while looking for a flat-screen television. *See, e.g., Galpin*,

720 F.3d at 447. However, this common-sense limit is much more difficult to apply in the digital realm, where responsive and non-responsive information is intermingled in computer storage.

Applying the plain view doctrine to searches of digital information presents serious and significant risks that law enforcement will be able to expand what should be limited, probable-cause based incursions into privacy into more generalized, unconstitutional searches. This Court should reject application of the plain view doctrine here.

**2. Reliance on the plain view doctrine to exploit an administrative overseizure is unreasonable in this case.**

Even if the plain view exception were applicable to searches of digital data, it would not justify the government’s search here. First, the plain view exception permits seizure of evidence only when an officer, during the course of a lawful search, comes “inadvertently across a piece of evidence incriminating the accused.” *Horton*, 496 U.S. at 135. Officers did not come across the evidence sought to be suppressed in the course of their lawful search pursuant to the July 2013 warrants. Rather, they found the evidence during a subsequent search entirely outside the scope of those warrants. “[A]n essential predicate of the plain view doctrine is that the initial intrusion [does] not violate the Fourth Amendment,” *Galpin*, 720 F.3d at 451 (quotation marks omitted)—and, as explained *supra* Part III, the March 2014 search exceeded the scope of the July 2013 warrants. *See Hughes*, 2020 WL 8022850, at \*17 n.25 (finding that the plain view exception did not apply to a cell phone search that “violate[d] the Fourth Amendment because it was not reasonably directed at uncovering evidence of the criminal activities alleged in the warrant”); *see also United States v. Gurczynski*, 76 M.J. 381, 388

(C.A.A.F. 2017) (“A prerequisite for the application of the plain view doctrine is that the law enforcement officers must have been conducting a lawful search when they stumbled upon evidence in plain view. As noted, the officers in this case were not [doing so] because the execution of the warrant was constitutionally unreasonable.”).

Second, it would violate Fourth Amendment reasonableness to allow the State to invoke plain view to take advantage of an administrative courtesy—its initial overseizure, allowed for the specific and limited purpose of permitting a reasonable search for information responsive to the July 2013 warrants—by later searching for and discovering new evidence it had never seen before his acquittal. *See, e.g., Thompson*, 28 N.Y.S. 3d 237; *Wey*, 256 F. Supp. 3d at 407. If this had not been a digital-search case, the government would never have possessed non-responsive material in the first place, let alone retained it up to and beyond his acquittal. But because the data in this case was digital in nature, the State could seize nonresponsive information, then exploit it after Mr. McCavitt’s acquittal to develop evidence of new criminal activity that it had never before seen or suspected to exist. Should the State prevail here, law enforcement will make this a regular practice. That is not the purpose of the plain-view exception to the warrant requirement.

**C. It was unreasonable for the State to re-search McCavitt’s data for evidence after his acquittal without obtaining a new warrant.**

Finally, the State’s failure to segregate responsive from non-responsive data on his hard drive, at least by the time its prosecution of McCavitt ended, was unreasonable under the Fourth Amendment. When the government seizes entire hard drives to facilitate particularized searches, the Fourth Amendment demands that it identify responsive data in a reasonable way, and within a reasonable amount of time. Here, examining the

“totality of the circumstances” and balancing McCavitt’s privacy interest in the non-responsive information on his hard drive against the State’s interest in searching that information without a new warrant, the Peoria P.D.’s March 2014 search violated the Fourth Amendment. *Samson v. California*, 547 U.S. 843, 848 (2006); *see Riley*, 573 U.S. at 385-86.

As explained above, McCavitt retained a strong privacy interest in the data on his hard drive even after the State seized and mirrored it. *See supra* Part I; *see also Hughes*, 2020 WL 8022850, at \*9; *contra* Pl. App. Br. 24 (relying on the “significantly reduced privacy and possessory interests in any copies of McCavitt’s hard drive”). And his privacy interest in data not described in the July 2013 warrants was *never* diminished before the Peoria P.D. searched it in March 2014.

On the other hand, the State’s interest in searching the drive without first obtaining a new warrant was miniscule—it could only seek evidence of the crime for which there was probable cause justifying the July 2013 warrants. And as to McCavitt’s *non-responsive* data—from which the evidence in this case was drawn—the State had no legitimate interest beyond administrative convenience to hold that data, and could only search it by demonstrating probable cause and obtaining a new warrant that authorized it to do so. *See supra* Part IV.A.

The question of whether the State lawfully *possessed* McCavitt’s hard drive even after his acquittal is beside the point. *See* Pl. App. Br. at 27-32. The proper question is not whether the State was legally required to give McCavitt his hard drive back (or delete its copies), but whether it was required, at the very least, to establish probable cause to justify its new invasion of McCavitt’s privacy and property interests and obtain a warrant

to exploit anew its possession of his private information. By the time of McCavitt's acquittal in March 2014, the State had effectuated its July 2013 warrants. It had searched the hard drive for responsive data, reviewed, identified, and processed evidence of the potential criminal activity discussed in those warrants, and fully and fairly litigated its charges to a jury verdict.

Once the jury acquitted, whatever authority the State possessed under the July 2013 warrants—namely investigation and possible prosecution of McCavitt for the specific criminal conduct within their scope—had expired. And the State's interest in diving back into the hard drive, without first obtaining a new warrant to authorize further searches, was especially small because—lawfully or not—it continued to possess the hard drive, entirely eliminating any risk of destruction or deletion.

The State attempts to focus the reasonableness analysis on its “interest in investigating” McCavitt based on its “susp[icion]” that McCavitt had “committ[ed] criminal conduct in addition to the conduct that resulted in the charges for which he was acquitted.” Pl. App. Br. 24. It also asserts that the State had a “pressing need to preserve access to defendant's computer data by retaining a copy” because of the possibility of spoliation. Pl. App. Br. 25. But to investigate new criminal conduct, the State's duty was simple: “get a warrant.” *Riley*, 573 U.S. at 403; *see supra* Part III.

## CONCLUSION

The Peoria P.D. violated the Fourth Amendment when it searched the copy of his hard drive without after his acquittal without probable cause and a valid warrant. Any evidence derived from that search should be suppressed. The judgment of the Court of Appeals should be affirmed.

Dated: March 3, 2021

Respectfully Submitted,

/s/ Rebecca K. Glenberg

Rebecca K. Glenberg  
ARDC No. 6322106  
Roger Baldwin Foundation of ACLU, Inc.  
150 N. Michigan Ave., Suite 600  
Chicago, IL 60601  
(312) 201-9740  
rglenberg@aclu-il.org  
*Counsel for Amici Curiae*

*On the Brief:*

Nusrat J. Choudhury  
Roger Baldwin Foundation of ACLU, Inc.  
150 N. Michigan Ave., Suite 600  
Chicago, IL 60601

Brett Max Kaufman  
Nathan Freed Wessler  
American Civil Liberties Union Foundation  
125 Broad Street  
New York, NY 10004

Jennifer Stisa Granick  
American Civil Liberties Union Foundation  
39 Drumm Street  
San Francisco, CA 94111

**CERTIFICATE OF COMPLIANCE**

I certify that this brief conforms to the requirements of Rules 345 and 341(a) and (b). The length of this brief, excluding the pages contained in the Rule 341(d) cover, the Rule 341(h)(1) table of contents and statement of points and authorities, the Rule 341(c) certificate of compliance, and the certificate of service, is 26 pages.

/s/ Rebecca K. Glenberg  
Rebecca K. Glenberg  
*Counsel for Amici Curiae*

**NOTICE OF FILING AND PROOF OF SERVICE**

The undersigned, an attorney, certifies that on March 3, 2021, she caused the foregoing **Motion for Leave and Brief of *Amici Curiae* American Civil Liberties Union and American Civil Liberties Union of Illinois in Support of Defendant-Appellee** to be filed with the Clerk of the Supreme Court of Illinois using the Court's electronic filing system and that the same was served by e-mail to the following counsel of record:

Leah M. Bendik  
Assistant Attorney General  
100 West Randolph Street, 12th Floor  
Chicago, Illinois 60601-3218  
(312) 814-5029  
eserve.criminalappeals@atg.state.il.us

Joshua B. Kutnick  
900 W Jackson Blvd., Suite 5W  
Chicago, IL 60607  
joshua@kutnicklaw.com

*Counsel for Defendant-Appellee*

*Counsel for Plaintiff-Appellant*

Within five days of acceptance by the Court, the undersigned also states that she will cause thirteen copies of the **Brief of *Amici Curiae*** to be mailed with postage prepaid to the following address:

Clerk of the Supreme Court of Illinois  
Supreme Court Building  
200 E. Capitol Ave  
Springfield, IL 62701

Under penalties as provided by law pursuant to Section 1-109 of the Code of Civil Procedure, the undersigned certifies that the statements set forth in this instrument are true and correct.

/s/ Rebecca K. Glenberg  
Rebecca K. Glenberg  
*Counsel for Amici Curiae*



2021 IL 125550

**IN THE  
SUPREME COURT  
OF  
THE STATE OF ILLINOIS**

---

(Docket No. 125550)

THE PEOPLE OF THE STATE OF ILLINOIS, Appellant, v.  
JOHN T. McCAVITT, Appellee.

*Opinion filed October 21, 2021.*

JUSTICE MICHAEL J. BURKE delivered the judgment of the court, with opinion.

Chief Justice Anne M. Burke and Justices Garman, Theis, Overstreet, and Carter concurred in the judgment and opinion.

Justice Neville dissented, with opinion.

**OPINION**

¶ 1 The Illinois State Police obtained warrants to seize and search a personal computer owned by defendant, John T. McCavitt, an officer of the Peoria Police Department. The warrant at issue in this appeal authorized law enforcement to

search the computer for digital evidence of two unrelated incidents: the aggravated criminal sexual assault of a named victim and the unauthorized video recording and live video transmission of an unnamed victim. Defendant was tried and acquitted of the alleged sexual assault before the unauthorized video recording was investigated.

¶ 2 Following defendant's acquittal and without seeking a new warrant, the Peoria Police Department acquired and searched a copy of the computer's hard drive, uncovering evidence of the unauthorized video recording. The digital search also uncovered child pornography, which was not mentioned in the warrant.

¶ 3 Based on the images, defendant was convicted of several counts of child pornography. The appellate court reversed the judgment on the ground that the search violated the fourth amendment (U.S. Const., amend. IV). 2019 IL App (3d) 170830, ¶ 32.

¶ 4 This appeal concerns the extent to which defendant's acquittal in the sexual assault proceedings affected his expectation of privacy in his computer data and whether the fourth amendment required the police to obtain a new warrant before searching the same data for evidence of another crime. The outcome turns on the interplay of four concepts: (1) a person's reasonable expectation of privacy in data on an electronic storage device that is subject to search, (2) double jeopardy principles, (3) the fourth amendment's particularity requirement as applied to electronic storage devices, and (4) the plain view doctrine.

¶ 5 In *People v. Hughes*, 958 N.W.2d 98, 104 (Mich. 2020) (*en banc*), the Michigan Supreme Court cogently explained that a search of an electronic storage device pursuant to a warrant must be reasonably directed at obtaining evidence relevant to the criminal activity alleged in the warrant. A search of digital data that is directed instead at uncovering evidence of criminal activity not identified in the warrant is effectively a warrantless search that violates the fourth amendment absent some exception to the warrant requirement. *Id.*

¶ 6 The warrant at issue diminished defendant's reasonable expectation of privacy in the images and videos he stored on his computer. When defendant was acquitted of the sexual assault, his reasonable expectation of privacy in his data relating to that offense was restored. However, the acquittal did not resolve the portion of the

warrant that authorized a search for digital evidence of the unauthorized video recording. The post-acquittal computer examination was reasonably directed at obtaining evidence of the unauthorized video recording, and the child pornography that was uncovered during the search was admissible because the images were found in plain view.

¶ 7 We hold that, under the unique facts of this case, the search that uncovered the child pornography did not violate defendant's fourth amendment rights. Therefore, we affirm the circuit's court's order denying defendant's motion to suppress the images and reverse the appellate court's judgment reversing that order.

¶ 8 I. BACKGROUND

¶ 9 This appeal is part of a series of three criminal prosecutions against defendant. All three are based on incriminating images and video uncovered on defendant's computer.

¶ 10 Defendant was charged in Peoria County case No. 13-CF-741 with aggravated criminal sexual assault (720 ILCS 5/11-1.30(a)(4) (West 2012)) and criminal sexual assault (*id.* § 11-1.20(a)(1)). Following defendant's acquittal in that case, the Peoria Police Department launched an internal investigation of defendant, which led to the discovery of additional incriminating images and video. The investigation was suspended when defendant was charged. He was ultimately convicted of (1) the unauthorized video recording of two women (Peoria County case No. 14-CF-203) and (2) child pornography in this case (Peoria County case No. 14-CF-282).

¶ 11 A. Peoria County Case No. 13-CF-741

¶ 12 Initially, defendant was investigated for criminal sexual assault against A.K., a female houseguest who was a friend and coworker of defendant's live-in girlfriend, Rachel Broquard. On July 17, 2013, the Illinois State Police obtained a warrant to search defendant's home for evidence of the alleged sexual assault, which defendant did not challenge.

¶ 13 The complaint for the warrant described A.K.'s account of the events. A.K. reported that defendant sexually assaulted her around 6 a.m. that day. A.K.,

Broquard, and defendant had gone out the previous night to celebrate with another coworker who was departing for graduate school. At approximately 4 a.m., A.K., Broquard, and defendant arrived at his residence and continued socializing. At 5:15 a.m., A.K. lay down, fully clothed, under the covers of a bed in a guest bedroom. A short time later, she awoke facedown wearing only her bra, which was pushed up. A.K. was in four-point restraints, and a black sleeping mask covered her head. She heard a “snap” that she believed to be from the cap of a lubricant container. A.K. also heard clicking noises that sounded like a camera shutter. Defendant sexually penetrated A.K. repeatedly and then released her from the restraints. A.K. quickly dressed, left the residence, and reported the incident.

¶ 14 The search warrant complaint alleged that digital evidence of criminal sexual assault could be found on defendant’s cellular phone. Accordingly, the warrant authorized the seizure of “any electronic media cable [*sic*] of video/audio recording” and “any electronic storage media capable of stor[ing] pictures, audio or video.” The warrant also authorized the seizure of any restraints that might have been used on the victim, physical evidence resulting from the assault, and any additional items of evidentiary value.

¶ 15 Officers of the Illinois State Police and the Peoria Police Department arrived at defendant’s home around 8:30 p.m. to execute the warrant. They waited two hours for defendant to answer the door and allow them inside. Defendant had called in sick to the police department that evening and had ignored telephone calls from his supervisors and the investigators. Defendant allegedly told Broquard that, while he kept the officers waiting outside, he removed the four-point restraints from the guest bedroom and placed them back under the mattress in the master bedroom.

¶ 16 The police officers seized defendant’s iPhone and his custom-built computer tower. The iPhone was found locked in a gun safe in the basement. The computer’s file history showed that more than 16,500 files had been recently deleted from the hard drive. The officers seized the restraints, a black blindfold, and lubricant. They also found a video recording system hidden inside two Kleenex tissue boxes.

¶ 17 An initial examination of the computer hard drive revealed photographs and video of A.K. lying motionless, facedown in four-point restraints. She was wearing only her top, which was pulled up, and a pillow covered her head. The officers

determined that the photographs and video of A.K. had been transferred from defendant's iPhone to his computer.

¶ 18 The initial examination of the hard drive also revealed what appeared to be secretly recorded video from defendant's bathroom of an unidentified woman stepping out of the shower. Defendant has not alleged that this initial examination of his computer data was unlawful.

¶ 19 On July 24, 2013, the Illinois State Police obtained a second warrant, which defendant also did not challenge. The warrant authorized "all peace officers in the state of Illinois" to search the computer for "any and all digital images, including, but not limited to JPG, GIF, TIF, AVI, MOV, and MPEG files" and "any evidence of" the offenses of (1) aggravated criminal sexual assault, (2) unlawful restraint, and (3) unauthorized video recording and live video transmission. The warrant authorized a search of "any and all stored/deleted data to determine which particular files are evidence or instrumentalities of criminal activity."

¶ 20 The search warrant complaint restated A.K.'s account of the events on July 17, 2013, but A.K. was not the only victim mentioned. The complaint specifically alleged that "[a]dditionally recovered videos display an unidentified female using the bathroom and taking a shower. The female appears to have no knowledge she was being recorded." Accordingly, the warrant authorized the search of defendant's computer for any evidence of the crimes listed "that may be discovered from separate incidents."

¶ 21 Detective Jeff Avery, a computer forensics expert with the Peoria County Sheriff's Department, examined defendant's computer. He removed the hard drive and made an exact, unalterable digital copy of its contents using EnCase software. Avery saved the copy, called the EnCase file, to his work computer. Avery reinstalled the hard drive and returned defendant's computer to the Illinois State Police.

¶ 22 Avery searched the EnCase file and found images relating to the incident involving A.K. On August 6, 2013, based on the images, the State charged defendant in Peoria County case No. 13-CF-741 with aggravated criminal sexual assault (720 ILCS 5/11-1.30(a)(4) (West 2012)) and criminal sexual assault (*id.*

§ 11-1.20(a)(1)) of A.K.<sup>1</sup> A jury ultimately found him not guilty of all charges on March 19, 2014.

¶ 23 Immediately following the not guilty verdicts, defense counsel orally requested the return of defendant’s personal property. Counsel specifically mentioned “collector guns” but did not ask for the computer. The trial court deferred ruling and asked counsel to file a written motion, because the seized items were weapons.

¶ 24 B. Internal Investigation of Defendant

¶ 25 The next day, on March 20, 2014, the Peoria Police Department initiated a formal investigation of defendant.<sup>2</sup> Detective James Feehan, a computer forensics examiner with the police department, requested and received a copy of the EnCase file from Avery.

¶ 26 On March 24, 2014, Feehan began a digital forensic analysis of the EnCase file and uncovered two images of what he believed to be child pornography. He also found video recordings of two unidentified women using the bathroom in defendant’s home. Feehan suspended his search to apply for a new warrant to further examine the EnCase file for child pornography.

¶ 27 Also on March 24, 2014, defendant filed a written motion in Peoria County case No. 13-CF-741, the sexual assault case, requesting the return of his property. The motion was silent as to the legal basis for the proposed disposition of defendant’s property. On April 24, 2014, the court ordered the return of defendant’s “guns + weapons instantanr” but otherwise continued the motion. The motion was never fully resolved, and defendant’s computer was not returned.

¶ 28 C. Peoria County Case No. 14-CF-203

¶ 29 On March 28, 2014, defendant was arrested and charged in Peoria County case No. 14-CF-203 with two counts of unauthorized video recording (720 ILCS 5/26-

---

<sup>1</sup>The July 24, 2013, warrant authorized a search for evidence of unlawful restraint—presumably committed against A.K.—but defendant was not charged with the offense.

<sup>2</sup>An arbitrator’s ruling and the police department’s collective bargaining agreement prohibited an internal investigation of defendant while the criminal case was pending.

4(a) (West 2014)) based on two incidents unrelated to the sexual assault charges. The pending criminal charges caused the Peoria Police Department to suspend its internal investigation of defendant.

¶ 30 The charges were based on the video recordings of two women, identified as Rachel G. and Whitney S., who were acquaintances of defendant and Broquard. *People v. McCavitt*, 2021 IL App (3d) 180399-U, ¶¶ 8-9. Defendant, using cameras concealed in the Kleenex boxes, secretly recorded the women using his bathroom. Defendant recorded Rachel on March 27, 2013, and recorded Whitney sometime between May 1, 2013, and the date his computer was seized.<sup>3</sup> Defendant transferred the video files to his computer.

¶ 31 D. Peoria County Case No. 14-CF-282

¶ 32 On April 1, 2014, Feehan obtained the new warrant to search the EnCase file for additional images of child pornography, which he uncovered soon thereafter. On April 28, 2014, the State filed a 10-count indictment, charging defendant with 7 counts of aggravated child pornography (720 ILCS 5/11-20.1B (West 2010)), a Class 2 felony, and 3 counts of child pornography (720 ILCS 5/11-20.1 (West 2012)), a Class 3 felony, based on five images found in the EnCase file.

¶ 33 On August 15, 2014, defendant filed a motion to suppress, arguing that Feehan had no authority to obtain and examine the contents of the EnCase file in March 2014. Defendant asserted that Feehan's examination was a warrantless search in violation of the fourth amendment because no criminal charges were pending at the time of the search. He also claimed the trial court in Peoria County case No. 13-CF-741, the sexual assault case, had erroneously failed to order the return of his computer and all copies of the hard drive, pursuant to section 108-2 of the Code of Criminal Procedure of 1963. See 725 ILCS 5/108-2 (West 2012).

¶ 34 Feehan testified at the suppression hearing that, as soon as he discovered the two pornographic images, he stopped to apply for a search warrant. He explained

---

<sup>3</sup>The State elected to prosecute the child pornography case first, but defendant ultimately was convicted of the two counts of unauthorized video recording. Defendant's convictions were affirmed on direct appeal. *McCavitt*, 2021 IL App (3d) 180399-U.

that the application process “took a couple days because we were investigating other unlawful videotaping evidence as part of that internal investigation.” On April 1, 2014, after obtaining the new warrant, Feehan resumed his search of the EnCase file and began looking specifically for child pornography.

¶ 35 Feehan testified that defendant had used White Canyon WipeDrive software, a utility program for permanently deleting data from a hard drive, at 9:23 p.m. on July 13, 2017, while the officers waited outside his home. However, Feehan was able to reconstruct how defendant had used the computer to search, download, and view child pornography from the Internet. Feehan referred to defendant’s work schedule to explain that defendant accessed the child pornography when he was off duty. Feehan recovered the file names of several permanently deleted images and videos that were labeled with child pornography acronyms, such as “PTHC,” meaning preteen hard core. Feehan was able to recover other files and identified their contents as child pornography.

¶ 36 Feehan pieced together the events during the hours between the alleged sexual assault and the computer seizure. Defendant called in sick to the police department at 6:01 p.m. Broquard used the computer for about 10 minutes, switched it off at 6:18 p.m., and went to work. At 6:26 p.m., defendant logged on as “owner,” and around 8:15 p.m. the police began knocking on defendant’s front door. Defendant deleted data from the computer from 9:18 p.m. to 10:07 p.m. Defendant allowed the police to enter around 10:30 p.m., at which time they seized the computer. Defendant was charged for the images that Feehan found despite defendant’s attempt to delete them permanently.

¶ 37 On cross-examination, Feehan testified that the Illinois State Police excluded him from the initial criminal investigation of the sexual assault to avoid a potential conflict of interest arising from Feehan and defendant sharing the same employer. Feehan conceded that he knew defendant had been acquitted of the sexual assault charges on March 19, 2014, and that no other charges were pending when he received the EnCase file from Avery on March 21, 2014. Feehan confirmed that he requested the EnCase file as part of the internal investigation even though he knew defendant’s computer had been seized in connection with the sexual assault prosecution.

¶ 38 Feehan testified, however, that at the time of his search, he “knew that there was [*sic*] other victims that could be identified during the formal [investigation] that would turn criminal.” Feehan did not believe he needed a search warrant or other court order to obtain and search the EnCase file “[b]ecause of case law that [he] was aware of” since defendant’s computer was previously seized “[p]ursuant to a lawful search warrant.”

¶ 39 On October 21, 2014, the trial court denied defendant’s motion to suppress, finding that law enforcement’s retention of defendant’s computer after the acquittal did not compel suppression of the child pornography. The court noted that defendant had not challenged (1) the warrants issued on July 17 and July 24, 2013, (2) the original search and seizure of his computer, or (3) Avery’s creation of the EnCase file. Regardless of whether the trial court in the sexual assault proceedings erred in failing to order the return of the computer, defendant had tried in that case to invoke section 108-2 of the Code of Criminal Procedure and had not alleged a fourth amendment violation. Moreover, returning the computer to defendant would not have prevented a search of the EnCase file, which Avery still possessed and had made available to Feehan. The trial court concluded that defendant’s suppression motion had raised an issue of search, not seizure. The seizure was presumptively reasonable because it was conducted pursuant to an unchallenged warrant, long before Feehan searched the EnCase file.

¶ 40 The trial court concluded that, once the police had the right to copy and examine the hard drive for evidence of certain crimes, defendant’s reasonable expectation of privacy in the information was substantially diminished but not totally frustrated. “[A]lthough the police had the right to search the hard drive for certain types of files and for evidence of certain types of offenses, the police did not have cart [*sic*] blanche to review everything on the hard drive.” For instance, the court noted, defendant still might have held expectations of privacy in a diary, daily planner, family history, drafts of papers for classes, and the like, but “he no longer held a ‘reasonable’ expectation of privacy in the types of files and directories which were or could be related to evidence of unlawful restraint and/or improper videotaping.”

¶ 41 The trial court found that Feehan did not violate defendant’s fourth amendment rights. Feehan’s search of files and folders for images and video did not exceed the scope of the original warrant because there was no testimony that the first two

images of child pornography were of a different file type or in different areas or directories of the computer than those previously subject to search under the warrant.

¶ 42 On July 10, 2015, the State amended its indictment and charged defendant with seven additional counts of child pornography (720 ILCS 5/11-20.1(a)(6) (West 2014)), a Class 2 felony, based on seven additional images found in the EnCase file.

¶ 43 A jury found defendant guilty of 15 of the 17 counts of child pornography. Defendant filed posttrial motions, which the trial court denied. The trial court accepted the jury's verdict on 1 count of Class 3 felony child pornography and 10 counts of Class 2 felony child pornography. The court sentenced defendant on the Class 3 felony to five years' imprisonment followed by mandatory supervised release of three years to life. The court imposed a sentence of 48 months' probation on the remaining 10 counts, to be served consecutively to the prison sentence.

¶ 44 On direct appeal, defendant argued, *inter alia*, that the trial court erroneously denied his motion to suppress. He argued that "Feehan's search of his EnCase file eight months after the initial warrant was issued and following his acquittal of sexual assault charges violated his fourth amendment rights." 2019 IL App (3d) 170830, ¶ 13. The Appellate Court, Third District, agreed and reversed the convictions.

¶ 45 The majority opinion concluded that, when the police took possession of defendant's computer, his expectation of privacy was significantly diminished until his sexual assault acquittal, which then triggered a statutory right to the return of his property and restored his expectation of privacy in the computer. *Id.* ¶ 24. The majority held that, although Avery created the EnCase file lawfully, Feehan violated defendant's right to privacy when he searched the file and found the first two images of child pornography. *Id.* ¶ 25. The police were not entitled to retain the entire EnCase file indefinitely but could examine it and retain only those files within the scope of the initial warrant. The majority held that, once defendant's sexual assault trial ended, the police were not entitled to retain any portion of the EnCase file, much less the entire file. *Id.* The majority concluded that, because the police had no authority to retain the EnCase file after defendant's acquittal, Feehan's initial search violated defendant's fourth amendment rights. *Id.* ¶ 26.

¶ 46 The majority also held that the images were not admissible under the good-faith exception to the exclusionary rule. *Id.* ¶ 31. Feehan, who had been a police officer for more than 20 years and a forensic examiner for 17 years, knew when he requested the EnCase file that defendant had been acquitted of the sexual assault charges and that no new charges had been filed. The majority concluded that, because the charges based on the files found pursuant to the initial warrant were no longer pending, Feehan should have known that the police had no right to retain, much less search, the EnCase file. *Id.* We note the majority opinion did not address the portion of the search warrant concerning the separate incident of unauthorized video recording.

¶ 47 The dissenting opinion concluded that defendant’s acquittal did not entitle him to the immediate return of his computer or the information harvested from it. *Id.* ¶ 37 (Wright, J., dissenting). The dissent noted that, after the acquittal, defendant did not pursue his oral and written requests for the return of his property. *Id.* ¶ 39. The dissent characterized the sexual assault court’s deferral of the oral request as a denial and concluded that the ruling stands as the law of the case and represents an unappealable order. *Id.* ¶ 40. The dissent also concluded that, because Feehan was merely reviewing information that had already been lawfully seized by another detective who had made it a part of his working file, defendant’s reasonable expectation of privacy remained diminished after he lawfully lost possession of the computer tower pursuant to the search warrant. *Id.* ¶ 44.

¶ 48 The State petitioned for leave to appeal, which we allowed pursuant to Illinois Supreme Court Rule 315(a) (eff. Oct. 1, 2019). We granted the American Civil Liberties Union and the American Civil Liberties Union of Illinois leave to submit briefs *amicus curiae* in support of defendant’s position, pursuant to Illinois Supreme Court Rule 345 (eff. Sept. 20, 2010).

¶ 49

## II. ANALYSIS

¶ 50

On appeal, the State argues Feehan’s examination of the EnCase file did not violate defendant’s fourth amendment rights because the search arose from the original lawful seizure and search of his computer. The State characterizes the search as a permissible “second look” that was no broader than the “first look” authorized by the original search warrant, which was broadly written,

unchallenged, and presumptively valid. The State also contends defendant's privacy and possessory interests in the EnCase file were so significantly reduced by the sexual assault prosecution that Feehan's examination did not even constitute a "search" under the fourth amendment. Third, the State asserts that, even if Feehan's examination qualifies as a warrantless search, the officer's review was reasonable because it constituted, at most, a minimal intrusion on defendant's privacy and possessory interests while diligently promoting compelling law enforcement interests. The State alternatively contends that the child pornography was admissible under the good-faith exception to the exclusionary rule.

¶ 51 Defendant renews his arguments that the child pornography should have been suppressed because Feehan's examination was a search that violated his expectation of privacy under the fourth amendment and that the images are not admissible under the good-faith exception to the exclusionary rule. Defendant also argues his property interest in the computer conferred a reasonable expectation of privacy in the data at the time of Feehan's search.

¶ 52 A. Standard of Review

¶ 53 We apply our familiar two-part standard of review to a ruling on a suppression motion. First, the circuit court's findings of historical fact should be reviewed only for clear error, and a reviewing court must give due weight to any inferences drawn from those facts by the fact finder. *People v. Luedemann*, 222 Ill. 2d 530, 542 (2006) (citing *Ornelas v. United States*, 517 U.S. 690, 699 (1996)). We defer to the court's factual findings and will reverse those findings only if they are against the manifest weight of the evidence. *Id.* (citing *People v. Sorenson*, 196 Ill. 2d 425, 431 (2001)). Second, a reviewing court may undertake its own assessment of the facts as they relate to the issues and may draw its own conclusions when deciding what relief should be granted. *Id.* (citing *People v. Pitman*, 211 Ill. 2d 502, 512 (2004)). Accordingly, the circuit court's ultimate legal ruling on the suppression motion is reviewed *de novo*. *Id.* As the relevant facts in this case are not in dispute, our review of the suppression ruling is *de novo*.

¶ 54

## B. Fourth Amendment

¶ 55

Defendant argued in his motion to suppress that Feehan’s examination violated his rights under the fourth amendment of the United States Constitution and article I, section 6, of the Illinois Constitution of 1970. The fourth amendment to the United States Constitution protects the “right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” U.S. Const., amend. IV; see also *Elkins v. United States*, 364 U.S. 206, 213 (1960) (the fourth amendment applies to state officials through the fourteenth amendment (U.S. Const., amend. XIV)). Similarly, article I, section 6, of the Illinois Constitution provides that the “people shall have the right to be secure in their persons, houses, papers and other possessions against unreasonable searches [and] seizures.” Ill. Const. 1970, art. I, § 6; see also 725 ILCS 5/108-7 (West 2012) (requiring the place or person to be searched and the items to be seized to be “particularly described in the warrant”). Under our limited lockstep doctrine, we construe the search and seizure clause of our state constitution in accordance with the United States Supreme Court’s interpretation of the fourth amendment unless any of the narrow exceptions to lockstep interpretation apply. *People v. Holmes*, 2017 IL 120407, ¶ 24. Defendant does not argue that an exception applies here.

¶ 56

The fourth amendment contains two separate clauses: the reasonableness clause and the warrant clause. U.S. Const., amend. IV; *Kentucky v. King*, 563 U.S. 452, 459 (2011). The reasonableness clause requires that all government searches and seizures be reasonable. *King*, 563 U.S. at 459; *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006) (the touchstone of fourth amendment analysis always is “reasonableness”). The warrant clause permits courts to issue warrants only if (1) the warrant is supported by probable cause and (2) the warrant includes particularized descriptions of “the place to be searched” and “the persons or things to be seized.” U.S. Const., amend. IV; *King*, 563 U.S. at 459. The second condition of the warrant clause is known as the particularity requirement.

¶ 57

A search warrant is not always required before searching or seizing a citizen’s personal effects (see *Stuart*, 547 U.S. at 403), but there is a “strong preference for searches conducted pursuant to a warrant” (*Illinois v. Gates*, 462 U.S. 213, 236 (1983)), and police officers generally must obtain a warrant for a search to be reasonable under the fourth amendment (see, e.g., *Riley v. California*, 573 U.S. 373,

382 (2014); *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (searches conducted outside the judicial process, without prior approval by a judge or magistrate, are *per se* unreasonable under the fourth amendment, subject only to a few specifically established and well-delineated exceptions).

¶ 58 C. Reasonable Expectation of Privacy in Digital Information

¶ 59 A search is constitutional if it does not violate a person’s “reasonable” or “legitimate” expectation of privacy. *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). To claim protection under the fourth amendment, a person must have exhibited an actual subjective expectation of privacy in the place searched or thing seized, and this expectation must be one that society is willing to recognize as reasonable. *People v. Rosenberg*, 213 Ill. 2d 69, 77 (2004). As in most cases, this appeal concerns whether defendant’s actual expectation of privacy was objectively reasonable.

¶ 60 There is no bright line rule indicating whether an expectation of privacy is constitutionally reasonable. See *O’Connor v. Ortega*, 480 U.S. 709, 715 (1987). Whether a defendant has a legitimate expectation of privacy in the place searched or the property seized thus depends on factors including (1) property ownership, (2) whether the defendant was legitimately present in the area searched, (3) the defendant’s possessory interest in the area searched or the property seized, (4) prior use of the area searched or property seized, (5) the ability to control or exclude others’ use of the property, and (6) a subjective expectation of privacy in the property. *People v. Lindsey*, 2020 IL 124289, ¶ 40. Whether a person’s expectation of privacy in an area searched is legitimate is determined by an objective standard drawn from common experience and based on the totality of the circumstances. *Id.*

¶ 61 In the context of the fourth amendment, computers and other electronic storage devices have historically been viewed as closed containers. Because individuals generally retain a reasonable expectation of privacy in the contents of a closed container that conceals its contents from plain view (see *United States v. Ross*, 456 U.S. 798, 822-23 (1982)), they also generally retain a reasonable expectation of privacy in data stored on electronic devices.

¶ 62            Accessing information stored in an electronic storage device will implicate the owner’s reasonable expectation of privacy in the information. *United States v. Heckenkamp*, 482 F.3d 1142, 1147 (9th Cir. 2007) (an individual generally has a reasonable expectation of privacy in their personal computers and data files). For instance, in *Riley*, the Supreme Court of the United States held that law enforcement generally must obtain a warrant before conducting a search of cell phone data. *Riley*, 573 U.S. at 386. The court described cell phones as “minicomputers that also happen to have the capacity to be used as telephones.” *Id.* at 393. Cell phones and personal computers share the notable distinguishing features of immense storage capacity and the ability to collect many distinct types of information, including a user’s Internet browsing history and “a cache of sensitive personal information” concerning nearly every aspect of a person’s life. *Id.* at 393-95.

“[A] cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.” (Emphasis omitted.) *Id.* at 396-97.

As the cell phone privacy concerns expressed in *Riley* apply to personal computers, we conclude that Feehan’s examination of the EnCase file constituted a search under the fourth amendment.

¶ 63            The State cites *United States v. Edwards*, 415 U.S. 800 (1974), for the proposition that the valid “first look” diminished defendant’s expectation of privacy and permitted Feehan’s examination. *Edwards* held that, when a person is lawfully arrested and taken into custody, the items in his possession when arrested—which were lawfully subject to search at the time and place of his arrest—may also be lawfully searched and seized without a warrant even though a “substantial period of time” has elapsed between the arrest and the time that the items are later searched. *Id.* at 807. *Edwards* does not apply because all the searches in this case were purportedly conducted pursuant to a warrant, not incident to defendant’s arrest. Furthermore, *Riley* instructs that law enforcement generally must obtain a warrant to search data on an electronic storage device, even if it was seized incident to arrest.

¶ 64

#### D. Defendant's Expectation of Privacy

¶ 65

Although an individual retains a reasonable expectation of privacy in a computer under his control, special circumstances may affect that expectation. In this case, the trial court correctly observed that defendant did not challenge the warrants authorizing the seizure of his computer, Avery's creation of the EnCase file, or Avery's subsequent search for digital evidence of the sexual assault. The unchallenged warrants made the initial seizure and search of defendant's computer presumptively reasonable.

¶ 66

Defendant, however, challenges Feehan's initial examination of the EnCase file, which uncovered evidence of the two incidents of unauthorized video recording and two images of child pornography. The State argues that Feehan's examination was not even a "search" under the fourth amendment because the initial warrant diminished defendant's privacy and possessory interests. In support, the State points out that the item searched was not the original hard drive but a copy that Avery created and stored on his work computer. The State asserts defendant did not have a legitimate expectation of privacy in the EnCase file because he did not create, own, or have lawful access to it. See *Lindsey*, 2020 IL 124289, ¶ 42.

¶ 67

The State focuses on defendant's lack of a formal property interest in the EnCase file itself and disregards defendant's informal privacy interest in his personal data. Defendant persuasively argues that "Feehan's examination of the police-generated forensic copy of [defendant's] original for information pertaining to a criminal investigation is no less a search and no less an infringement on his property rights than had Feehan examined the original." The right to exclude others is one of the main rights attaching to property, and allowing access to a copy defeats that right. See *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978); see also *United States v. Jefferson*, 571 F. Supp. 2d 696, 702 (E.D. Va. 2008) ("the Fourth Amendment protects an individual's possessory interest in information itself," and copying interferes with the owner's possession and interest in privacy of the information contained in the documents).

¶ 68

The evidentiary value of data resides in the data itself, not in the medium on which it is stored. To suggest that defendant lacked an expectation of privacy in the contents of his personal computer because those contents were copied to another medium contravenes the requirement of reasonableness, which is the touchstone of

any fourth amendment analysis. See *Stuart*, 547 U.S. at 403. “[I]maging a computer should be regulated by the Fourth Amendment and searches of copies should be treated the same as searches of the original” (Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 532 (2005)) because “computers work by copying and recopying information” (*id.* at 564). Treating a digital copy as the original recognizes that the key to fourth-amendment reasonableness is the access to data, regardless of whether the data is copied, transferred, or otherwise manipulated. *Id.*

¶ 69 We agree with defendant that his privacy interest in the computer’s contents extended to the EnCase file. But he goes further, asserting his property interest in the data obviates the need to show an expectation of privacy. He claims “[h]e is not required to prove that he had an expectation of privacy in his computer, his hard drive, the forensic duplicate of the hard drive, or his personal information stored on these electronic devices in order to show that the police performed a search.” Defendant’s property interest in the data is not dispositive of the search’s reasonableness, otherwise mere proof of ownership in a place or item to be searched would be sufficient for suppression.

¶ 70 To summarize, defendant’s privacy interests in the original hard drive and the EnCase file were the same. However, the privacy interest conferred by his ownership of the computer is not dispositive to our inquiry. The appeal turns on defendant’s privacy interest in light of the warrant and the reasonableness of Feehan’s examination of the EnCase file following defendant’s acquittal in the sexual assault proceeding.

¶ 71 E. Restoration of Defendant’s Expectation of Privacy

¶ 72 Defendant argues that, once he was acquitted in the sexual assault case, (1) he was entitled by statute to the return of his property, (2) his expectation of privacy in the computer was restored, and (3) it was unreasonable for law enforcement to look at the data without obtaining a new warrant. We conclude that defendant’s acquittal only partially restored his reasonable expectation of privacy in his computer.

¶ 73

## 1. Criminal Sexual Assault

¶ 74

The parties do not dispute that defendant's sexual assault trial culminated in an acquittal for double jeopardy purposes. An acquittal triggers the double jeopardy clause of the fifth amendment to the United States Constitution, which provides that no person shall "be subject for the same offence to be twice put in jeopardy of life or limb." U.S. Const., amend. V. Similarly, article I, section 10, of the Illinois Constitution provides that no person shall "be twice put in jeopardy for the same offense." Ill. Const. 1970, art. I, § 10. The prohibition against double jeopardy is animated by the principle that

" 'the State with all its resources and power should not be allowed to make repeated attempts to convict an individual for an alleged offense, thereby subjecting him to embarrassment, expense and ordeal and compelling him to live in a continuing state of anxiety and insecurity, as well as enhancing the possibility that even though innocent he may be found guilty.' " *People v. Williams*, 188 Ill. 2d 293, 307 (1999) (quoting *Green v. United States*, 355 U.S. 184, 187-88 (1957)).

¶ 75

"The prohibition against double jeopardy 'protects against three distinct abuses: (1) a second prosecution for the same offense after acquittal; (2) a second prosecution for the same offense after conviction; and (3) multiple punishments for the same offense.' " *People v. Henry*, 204 Ill. 2d 267, 283 (2003) (quoting *People v. Placek*, 184 Ill. 2d 370, 376-77 (1998)); see also *United States v. Wilson*, 420 U.S. 332, 343 (1975). "An acquittal triggers the bar against double jeopardy only if the acquittal 'actually represents a resolution, correct or not, of some or all of the factual elements of the offense charged.' " *Henry*, 204 Ill. 2d at 283 (quoting *United States v. Martin Linen Supply Co.*, 430 U.S. 564, 571 (1977)).

¶ 76

When the jury found defendant not guilty of aggravated criminal sexual assault and criminal sexual assault, the verdicts represented a resolution of the factual elements of the offenses charged. The bar against double jeopardy protected defendant against a second prosecution for those offenses, restoring defendant's reasonable expectation of privacy concerning the data that constituted evidence of those crimes. Defendant, newly freed from "a continuing state of anxiety and insecurity" that he would be retried for sexual assault (*Williams*, 188 Ill. 2d at 307),

regained a reasonable expectation that the police would not search his computer for evidence of the offenses of which he was acquitted.

¶ 77 Defendant renews his argument that the acquittal entitled him to the return of his computer and to any copies of his personal data and that therefore his reasonable expectation of privacy in the data was restored *entirely*. We disagree. To establish a legitimate expectation in the place to be searched, a defendant must point to a source outside the constitution—namely, formal property interests or informal privacy interests. *United States v. Jones*, 565 U.S. 400, 408 (2012); *Rakas*, 439 U.S. at 143 n.12 (“Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.”).

¶ 78 Defendant asserts his formal property interests in the computer, relying on section 108-2 of the Code of Criminal Procedure, which governs the return of property after a person is released from custody. But the statute applies to items seized *without* a warrant, stating

“An inventory of all instruments, articles or things *seized on a search without warrant* shall be given to the person arrested and a copy thereof delivered to the judge before whom the person arrested is taken, and thereafter, such instruments, articles or things shall be handled and disposed of in accordance with Sections 108-11 and 108-12 of this Code. If the person arrested is released without a charge being preferred against him all instruments, articles or things seized, other than contraband, shall be returned to him upon release.” (Emphasis added.) 725 ILCS 5/108-2 (West 2012).

¶ 79 Section 108-2 arguably did not apply to defendant’s computer because the statute applies to “things seized without a warrant.” Defendant’s acquittal does not negate the fact that the defendant’s computer was seized on July 17, 2013, pursuant to a warrant.

¶ 80 In contrast to section 108-2, section 108-10 applies to items seized *with* a warrant, like defendant’s computer. Section 108-10 provides for the items seized by law enforcement to be returned to the court:

“A return of all instruments, articles or things seized shall be made without unnecessary delay before the judge *issuing the warrant* or before any judge *named in the warrant* or before any court of competent jurisdiction. An inventory of any instruments, articles or things seized shall be filed with the return and signed under oath by the officer or person *executing the warrant*. The judge shall upon request deliver a copy of the inventory to the person from whom or from whose premises the instruments, articles or things were taken and to the *applicant for the warrant*.” (Emphases added.) *Id.* § 108-10.

¶ 81 Regardless of which statute governed the custody of defendant’s computer, we agree with the trial court and the dissenting appellate opinion that defendant failed to invoke any authority for the return of his computer or copies of its hard drive. In fact, defendant states in his brief that his “items have never been returned,” but he does not accuse the State of any wrongdoing.

¶ 82 Moreover, defendant cites no authority to suggest that his acquittal automatically entitled him to the immediate return of his computer and the information harvested from it. In fact, section 108-11 provides that “[t]he court before which the instruments, articles or things are returned shall enter an order providing for their custody pending further proceedings.” *Id.* § 108-11. Thus, the statute contemplates a motion and a hearing before an order is entered disposing of seized items. See, *e.g.*, *City of Chicago v. Pudlo*, 123 Ill. App. 3d 337, 345 (1983) (order denying defendants’ motion for return of weapons was reversed because trial court erroneously failed to conduct hearing). Here, the State argued at the suppression hearing that, if defendant had noticed up his motion, the State would have opposed the return of the computer to defendant on the ground that the hard drive contained contraband. In any event, the record indicates that defendant neither pursued his written motion for the return of his computer nor appealed any order in Peoria County case No. 13-CF-741.

¶ 83 Defendant asserts a possessory interest in the computer and claims it extends to the digital copies of the hard drive, but the trial court never reached the issue, which was governed by statute and was subject to an evidentiary hearing. As defendant did not press his rights in the sexual assault proceeding, he cannot claim his property interest fully restored his expectation of privacy in his data.

¶ 84

## 2. Unauthorized Video Recording

¶ 85

The acquittal resolved the portion of the July 24, 2013, search warrant that was directed toward the offense of aggravated criminal sexual assault. However, the acquittal did not resolve any of the factual elements of unauthorized video recording, which was also specified in the warrant. Contrary to defendant's suggestion, the acquittal did not nullify the warrant entirely. The State concludes that the sexual assault acquittal did not restore defendant's expectation of privacy concerning evidence of the uncharged offenses described in the July 24, 2013, warrant, including unauthorized video recording.

¶ 86

Defendant responds that the State has forfeited the issue. *Village of Lake Villa v. Stokovich*, 211 Ill. 2d 106, 121 (2004) (issues not raised in the trial court generally are forfeited and may not be raised for the first time on appeal). Defendant cites the appellate majority's observation that "[t]he State concedes that the *July 17, 2013*, warrant 'did not authorize Feehan's search, as that warrant had already been executed and, after investigation and criminal proceedings, defendant was acquitted.'" (Emphasis added.) 2019 IL App (3d) 170830, ¶ 30. But the State has argued throughout the proceedings that the *July 24, 2013*, warrant authorized Feehan's search.

¶ 87

For instance, the State argues in its opening brief that it had an ongoing interest in investigating defendant because, "based on prior searches of defendant's computer data, phone data, and email account, the [Peoria Police Department] suspected defendant of committing criminal conduct in addition to the conduct that resulted in the charges for which he was acquitted." The State narrows its argument in the reply brief, asserting that the search warrant described "separate incidents" besides the sexual assault of A.K. We consider the issue adequately preserved. *Dillon v. Evanston Hospital*, 199 Ill. 2d 483, 504-05 (2002) (the forfeiture rule is an admonition to the parties and not a limitation on the jurisdiction of this court).

¶ 88

### F. Scope of the Warrant

¶ 89

The validity of Feehan's search depends on whether it was within the scope of the portion of the warrant that was unresolved by the acquittal. It is well established that a search warrant need not contain " '[a] minute and detailed description of the

property to be seized.’ ” *People v. McCarty*, 223 Ill. 2d 109, 151 (2006) (quoting *People v. Prall*, 314 Ill. 518, 523 (1924)). “Rather, ‘the property must be so definitely described that the officer making the search will not seize the wrong property.’ ” *Id.* (quoting *Prall*, 314 Ill. at 523). When a type of property, rather than particular property, is to be seized, a description of its characteristics is sufficient. *Id.* at 152.

¶ 90 The Michigan Supreme Court has recently explained how the fourth amendment’s particularity requirement applies to digital evidence. In *Hughes*, the defendant was under investigation for drug trafficking, and law enforcement obtained a warrant to search his cell phone for evidence related to separate criminal allegations of that crime. *Hughes*, 958 N.W.2d at 105. The warrant affidavit contained no information concerning armed robbery. *Id.* The warrant provided that “ ‘[a]ny cell phones or \*\*\* other devices capable of digital or electronic storage seized by authority of this search warrant shall be permitted to be forensically searched and or manually searched, and any data that is able to be retrieved there from shall be preserved and recorded.’ ” *Id.* The warrant authorized the seizure of any drug paraphernalia and “ ‘any records pertaining to the receipt, possession and sale or distribution of controlled substances including but not limited to documents, video tapes, computer disks, computer hard drives, and computer peripherals.’ ” (Emphasis omitted.) *Id.* at 106.

¶ 91 After the cell phone was seized, the defendant was charged with an armed robbery that occurred a week before the warrant was issued. *Id.* The police examined the phone and extracted all the data. About a month after the extraction and at the request of the prosecutor in the armed-robbery case, a detective searched the cell-phone data again. *Id.* The searches uncovered evidence of the defendant’s involvement in the armed robbery, and the evidence was used to convict the defendant of armed robbery. *Id.* at 106-07.

¶ 92 On appeal from the armed-robbery conviction, the defendant argued that “the phone records should have been excluded from trial because the warrant supporting a search of the data only authorized a search for evidence of drug trafficking and not armed robbery.” *Id.* at 107. The Michigan Supreme Court agreed, concluding that the seizure and search of cell-phone data pursuant to a warrant does not

extinguish the “otherwise reasonable expectation of privacy in the entirety of that seized data.” *Id.* at 111. Specifically, the *Hughes* court held

“the police were permitted to seize and search that data, but only to the extent authorized by the warrant. Any further review of the data beyond the scope of that warrant constitutes a search that is presumptively invalid under the Fourth Amendment, absent some exception to that amendment’s warrant requirement.” *Id.* at 115.

¶ 93 The *Hughes* court then considered “whether the review of [the] defendant’s data for evidence of an armed robbery fell within the scope of the warrant issued in the drug-trafficking case.” *Id.* The court held that a search of cell-phone data “must be ‘reasonably directed at uncovering’ evidence of the criminal activity alleged in the warrant and that any search that is not so directed but is directed instead toward finding evidence of other and unrelated criminal activity is beyond the scope of the warrant.” (Emphasis omitted.) *Id.* (quoting *United States v. Loera*, 923 F.3d 907, 917 (10th Cir. 2019)).

¶ 94 The court acknowledged that a “criminal suspect will not always store or organize incriminating information on his or her digital devices in the most obvious way or in a manner that facilitates the location of that information.” *Id.* at 117. Nonetheless, the court declined

“to adopt a rule that it is always reasonable for an officer to review the entirety of the digital data seized pursuant to a warrant on the basis of the mere possibility that evidence may conceivably be found anywhere on the device or that evidence might be concealed, mislabeled, or manipulated.” *Id.*

¶ 95 “Such a per se rule would effectively nullify the particularity requirement of the Fourth Amendment in the context of cell-phone data and rehabilitate an impermissible general warrant that ‘would in effect give “police officers unbridled discretion to rummage at will among a person’s private effects.” ’ ” (Emphasis omitted.) *Id.* at 118 (quoting *Riley*, 573 U.S. at 399, quoting *Gant*, 556 U.S. at 345). An officer’s search of seized digital data, as with any other search conducted pursuant to a warrant, must be reasonably directed at finding evidence of the criminal activity identified within the warrant. *Id.*

¶ 96

The *Hughes* court explained that the test in the digital context is whether the forensic steps of the search process were reasonably directed at uncovering the evidence specified in the search warrant. *Id.* Whether a data search that uncovers evidence of criminal activity not identified in the warrant was reasonably directed at finding evidence relating to the criminal activity alleged in the warrant turns on a number of considerations, including (1) the nature of the criminal activity alleged and the type of digital data likely to contain evidence relevant to the alleged activity; (2) the evidence provided in the warrant affidavit for establishing probable cause that the alleged criminal acts have occurred; (3) whether nonresponsive files are segregated from responsive files on the device; (4) the timing of the search in relation to the issuance of the warrant and the trial for the alleged criminal acts; (5) the technology available to allow officers to sort data likely to contain evidence related to the criminal activity alleged in the warrant from data not likely to contain such evidence without viewing the contents of the unresponsive data and the limitations of this technology; (6) the nature of the digital device being searched; (7) the type and breadth of the search protocol employed; (8) whether there are any indications that the data has been concealed, mislabeled, or manipulated to hide evidence relevant to the criminal activity alleged in the warrant, such as when metadata is deleted or when data is encrypted; and (9) whether, after reviewing a certain number of a particular type of data, it becomes clear that certain types of files are not likely to contain evidence related to the criminal activity alleged in the warrant. *Id.* at 118-20.

“To be clear, a court will generally need to engage in such a ‘totality-of-circumstances’ analysis to determine whether a search of digital data was reasonably directed toward finding evidence of the criminal activities alleged in the warrant only if, while searching digital data pursuant to a warrant for one crime, officers discover evidence of a different crime without having obtained a second warrant and a prosecutor seeks to use that evidence at a subsequent criminal prosecution.” *Id.* at 120.

¶ 97

The *Hughes* court found the search for armed robbery evidence was outside the scope of the warrant, which authorized a data search only for evidence of drug trafficking and “did not even mention” the armed robbery or its surrounding circumstances. *Id.* at 121. The second search of the phone violated the fourth amendment because the “review was directed exclusively toward finding evidence

related to the armed-robbery charge, and it was grounded in information obtained during investigation into that crime.” (Emphasis omitted.) *Id.* at 122.

¶ 98 We are persuaded by *Hughes* that an officer’s search of seized digital data, as with any other search with a warrant, must be reasonably directed at finding evidence of the criminal activity identified within the warrant.

¶ 99 The warrants in this case and in *Hughes* make the cases factually distinguishable. The *Hughes* warrant authorized a data search for evidence of drug trafficking, but the supporting affidavit did not mention armed robbery, let alone claim probable cause that the defendant committed armed robbery. As a result, the warrant did not authorize a search for digital evidence related to the armed robbery.

¶ 100 By contrast, the search warrant in this case was not limited to uncovering evidence of the sexual assault of which defendant was acquitted. The July 24, 2013, warrant also authorized a search for digital evidence of unauthorized video recording. Double jeopardy protected defendant from retrial on the sex offenses, but defendant still could be charged with unauthorized video recording, because the issuing court found there was probable cause to search defendant’s data for evidence of that offense.

¶ 101 The *Hughes* factors indicate Feehan’s search was reasonably directed at finding evidence of the unauthorized video recording. Specifically, the complaint for the July 24, 2013, search warrant stated that “[a]dditionally recovered videos display an unidentified female using the bathroom and taking a shower” and that this “unidentified female appears to have no knowledge she was being recorded.” The complaint expressly targeted the crime of “Unauthorized Video Recording/Live Video Transmission in violation of 720 ILCS 5/26-4,” and the warrant authorized the search of all digital images for “Unauthorized Video Recording/Live Video Transmission 720 ILCS 5/26-4.”

¶ 102 The warrant permitted a search of “any and all digital images, including, but not limited to JPG, GIF, TIF, AVI, MOV, and MPEG files,” which are image and video file formats likely to contain evidence relevant to unauthorized video recording. Moreover, the evidence provided in the search warrant application described the bathroom video in sufficient detail to establish probable cause. Defendant has not challenged Feehan’s methodology concerning search protocols

and the sorting of responsive and unresponsive data, and Feehan testified to defendant's attempts to hide relevant evidence by permanently deleting files. See *Hughes*, 958 N.W.2d at 118.

¶ 103 The concurring opinion in *Hughes* stated that an officer's subjective intention in conducting the search also should be considered as a potentially dispositive factor in determining whether the search of seized data is reasonably directed at finding evidence of the criminal activity identified in the warrant. *Id.* at 124 (Viviano, J., concurring). The concurrence concluded that, if the officer purposefully searches for evidence of a crime other than the one identified in the warrant, the search cannot be reasonably directed at uncovering evidence of the criminal activity alleged in the warrant. *Id.* at 124-25.

¶ 104 Feehan's conduct adhered to the special concurrence in *Hughes*. Feehan testified at the suppression hearing that he was not searching for evidence of the criminal sexual assault, because defendant already had been acquitted of that charge. But contrary to defendant's assertion, the detective did not engage in a fishing expedition. Feehan testified that "we were investigating other unlawful videotaping evidence as part of [the] internal investigation" and that he "knew that there was [*sic*] other victims" besides A.K. Also, Feehan actually uncovered evidence of the offense described in the warrant. The July 24, 2013, warrant authorized law enforcement to search for digital evidence of the unauthorized video recording of another victim, and Feehan's search and subjective intent were consistent with the warrant.

¶ 105 G. Timeliness of Search

¶ 106 Defendant primarily argues that his acquittal restored his expectation of privacy in all the data, but he also suggests that Feehan's search was unreasonable because it was conducted eight months after the warrant was issued. Following the acquittal, the warrant still authorized a search for evidence of unauthorized video recording, and as the appellate majority noted, the fourth amendment does not place explicit limits on the duration of any forensic analysis authorized by a warrant. 2019 IL App (3d) 170830, ¶ 19 (" 'under current law there is no established upper limit as to when the government must review seized electronic data to determine whether the

evidence seized falls within the scope of a warrant.’ ” (quoting *United States v. Metter*, 860 F. Supp. 2d 205, 215 (E.D.N.Y. 2012))).

¶ 107 Courts have upheld forensic analyses begun months after law enforcement acquires the electronic storage device. See *United States v. Syphers*, 426 F.3d 461, 469 (1st Cir. 2005) (a five-month delay in processing a computer already in police custody “did not invalidate the search \*\*\* because there is no showing that the delay caused a lapse in probable cause, that it created prejudice to the defendant, or that federal or state officers acted in bad faith to circumvent federal requirements”); *United States v. Burns*, No. 07 CR 556, 2008 WL 4542990, at \*8-9 (N.D. Ill. Apr. 29, 2008) (10-month delay); *United States v. Gorrell*, 360 F. Supp. 2d 48, 55 n.5 (D.D.C. 2004) (10-month delay for off-site forensic analysis). The fourth amendment does not subject data searches to any rigid time limit because they may involve much more information than an ordinary document search and require more preparation and a greater degree of care in their execution. 2019 IL App (3d) 170830, ¶ 19 (citing *United States v. Triumph Capital Group, Inc.*, 211 F.R.D. 31, 66 (D. Conn. 2002)). Nevertheless, the fourth amendment requires the government to complete its review of digital data “ ‘within a “reasonable” period of time.’ ” *Id.* (quoting *Metter*, 860 F. Supp. 2d at 215). A search of digital data that takes several years may be reasonable as long as the search ends before trial and does not exceed the scope of the original search warrant. See *United States v. Johnston*, 789 F.3d 934, 942-43 (9th Cir. 2015).

¶ 108 We agree with defendant that the acquittal eliminated the probable cause to search for evidence of the sexual assault. But to the extent that defendant argues the eight-month delay in conducting the search was unreasonable, he does not claim that probable cause to search for unauthorized video recording dissipated while the sexual assault prosecution was pending, nor could he, because his data remained secured and unaltered in the EnCase file. He also does not claim prejudice by the delay or that the police department acted in bad faith. See *Burns*, 2008 WL 4542990, at \*9 (search upheld despite “lengthy” delay because the defendant did not assert that “the time lapse affected the probable cause to search the computer (nor could he, given that suspected child pornography had already been found on the hard drive), that the government has acted in bad faith, or that he has been prejudiced in any way by the delay”); see also *Syphers*, 426 F.3d at 469 (the fourth amendment “ ‘contains no requirements about when the search or seizure is to occur

or the duration’ ” (quoting *United States v. Gerber*, 994 F.2d 1556, 1559-60 (11th Cir. 1993)), but “ ‘unreasonable delay in the execution of a warrant that results in the lapse of probable cause will invalidate a warrant’ ” (quoting *United States v. Marin-Buitrago*, 734 F.2d 889, 894 (2d Cir. 1984)). The passage of eight months from the warrant issuance to Feehan’s search was reasonable under the circumstances, considering the intervening sexual assault prosecution, which required the police department to delay its internal investigation, and the sheer volume of data in the EnCase file.

¶ 109

#### H. Plain View

¶ 110

*Hughes* contrasted its facts with

“a circumstance in which the officer was reasonably reviewing data for evidence of drug trafficking and happened to view data implicating defendant in other criminal activity. If such were the case and the data’s ‘incriminating character [was] immediately apparent,’ the plain-view exception would likely apply and permit the state to use the evidence of criminal activity not alleged in the warrant at a subsequent criminal prosecution.” *Hughes*, 958 N.W.2d at 122.

The court’s hypothetical matches this case.

¶ 111

Evidence of a crime may be seized without a warrant under the plain view exception to the warrant requirement. A police officer may properly seize evidence of a crime without a warrant if (1) the officer was lawfully in a position from which to view the object seized in plain view, (2) the object’s incriminating character was immediately apparent, meaning the officer had probable cause to believe the object was contraband or evidence of a crime, and (3) the officer had a lawful right of access to the object itself. *Horton v. California*, 496 U.S. 128, 134-36 (1990). However, “the ‘plain view’ doctrine may not be used to extend a general exploratory search from one object to another until something incriminating at last emerges.” *Coolidge v. New Hampshire*, 403 U.S. 443, 466 (1971).

¶ 112

This case presents the most common use of the plain view doctrine in the context of digital data, which occurs when law enforcement examines a computer pursuant to a search warrant and discovers evidence of a separate crime that falls

outside the scope of the search warrant. The inquiry focuses on whether an officer is exploring hard drive locations and opening files responsive to the warrant, considering both the types of files accessed and the crimes specified in the warrant. *Johnston*, 789 F.3d at 941-43. For example, in *United States v. Wong*, 334 F.3d 831, 838 (9th Cir. 2003), an agent uncovered child pornography on a hard drive while conducting a valid search of the drive for evidence of a murder. Because the agent was properly searching graphics files for evidence of the murder, the child pornography was properly seized and subsequently admitted under the plain view doctrine. *Id.*

¶ 113 We agree with the State that the child pornography was admissible under the plain view doctrine, despite the warrant seeking evidence related to unauthorized video recording. The July 24, 2013, warrant authorized Feehan to search the EnCase file for evidence of the unauthorized video recording, including “any and all digital images, including, but not limited to JPG, GIF, TIF, AVI, MOV, and MPEG files.” Feehan testified that the child pornography was in the JPG file format. The trial court found there was no testimony that the first two images of child pornography were of a different file type or in different areas or directories of the computer than those previously subject to search under the warrant. Defendant does not quarrel with the court’s finding, which is not against the manifest weight of the evidence.

¶ 114 Defendant does not allege that Feehan accessed an area of the hard drive that fell outside the scope of the warrant or that Feehan would have reason to know, before opening the digital images, that they would not contain evidence of the crimes listed on the warrant. Feehan had lawful access to the EnCase file to search for images and video of unauthorized video recording, and he testified that the incriminating character of the two JPG files containing the child pornography was immediately apparent, meaning he had probable cause to believe the files were evidence of a crime. See *Horton*, 496 U.S. at 134. Finding the first two images caused Feehan to suspend his search before securing another warrant to search for additional images of child pornography.

¶ 115 As Feehan’s search was within the scope of the July 24, 2013, warrant and the images of child pornography were admissible under the plain view doctrine, we need not address the State’s alternate argument that the child pornography was

admissible under the good-faith exception to the warrant requirement.

¶ 116

### III. CONCLUSION

¶ 117

To summarize, the warrant authorizing the search of defendant's computer data diminished his expectation of privacy in the types of files described in the warrant. However, any postacquittal search of the same data, directed toward uncovering further evidence of the sexual assault, would have exceeded the scope of the warrant. In this case, Feehan's data search was within the scope of the warrant because it was reasonably directed at uncovering evidence of unauthorized video recording, which was alleged in the warrant. Feehan's search was not directed at finding evidence of criminal activity not described in the warrant. Therefore, the search was reasonable under the fourth amendment and resulted in the lawful discovery of child pornography in plain view.

¶ 118

For the preceding reasons, we hold that the appellate court erred in reversing the trial court's denial of defendant's motion to suppress evidence. We reverse the judgment of the appellate court and affirm the trial court's denial of defendant's motion to suppress the digital images supporting his convictions of child pornography.

¶ 119

Appellate court judgment reversed.

¶ 120

Circuit court judgment affirmed.

¶ 121

JUSTICE NEVILLE, dissenting:

¶ 122

In this case, the majority holds that the police did not violate McCavitt's privacy rights after his acquittal for criminal sexual assault when they searched a copy of the data on his computer hard drive on March 24, 2014, with a search warrant issued on July 24, 2013, because (1) McCavitt's acquittal of criminal sexual assault (a) only partially restored his right to privacy in his computer data involving charges of criminal sexual assault but (b) his acquittal did not restore his privacy rights in evidence of the second offense listed in the July 24, 2013, search warrant—an unauthorized video recording—and (2) police conducted the March 24, 2014,

search within a “reasonable time” after the circuit court issued the July 24, 2013, search warrant.

¶ 123 I agree with the majority that McCavitt had a reasonable expectation of privacy in the data on his computer hard drive. *Supra* ¶ 69. I also agree with the majority that McCavitt’s March 19, 2014, acquittal affected his privacy rights in his property. *Supra* ¶ 70. I disagree with the majority that (1) the search warrant issued on July 24, 2013, remained valid for 243 days until March 24, 2014, for searches for evidence of crimes for which McCavitt was not acquitted that were listed in the July 24, 2013, search warrant and (2) the police could lawfully remain in possession of McCavitt’s hard drive data for 243 days (from July 24, 2013, until March 24, 2014) before the hard drive was searched for data.

¶ 124 I would find that the State’s March 24, 2014, search of McCavitt’s data violated his constitutional and statutory rights for three reasons: (1) McCavitt had a constitutional right to privacy in the personal data on his hard drive and his right to privacy cannot be interfered with or intruded upon without a valid warrant issued after a showing of probable cause; (2) section 108-6 of the Code of Criminal Procedure of 1963 (Code) (725 ILCS 5/108-6 (West 2020)) gave the police 96 hours to execute the July 24, 2013, search warrant and search McCavitt’s hard drive for data, and once the 96 hours expired the search warrant was void (*id.*); and (3) once McCavitt was acquitted on March 19, 2014, section 108-11 of the Code mandated that the trial judge enter an order directing the State to return McCavitt’s property (*id.* § 108-11). Accordingly, I respectfully dissent.

¶ 125 **BACKGROUND**

¶ 126 On July 17, 2013, the circuit court issued its first warrant to search the single-family residence located at 1710 W. West Aire Avenue in Peoria, Illinois, and the Illinois State Police (ISP) executed the warrant and seized McCavitt’s computer and hard drive.

¶ 127 On July 24, 2013, the circuit court issued its second warrant, at 2:05 p.m., to “search and examine in greater detail” (1) a telephone possessing telephone number (309) 657-4\*\*\* and (2) an LG Computer Tower SN No. WMAZA2914641 that were seized on July 17, 2013, for digital images, for stored and deleted data, for

evidence of criminal activity, and for any evidence of aggravated criminal sexual assault, unlawful restraint, or unauthorized video recording.

¶ 128 The parties stipulated that on July 25, 2013, the ISP transported McCavitt's hard drive to Detective Jeff Avery, a member of the Peoria County Sheriff's Department (PCSD) and a forensic examiner on special assignment to the U.S. Attorney's office. Detective Avery testified that he removed the hard drive from McCavitt's computer, copied it, and saved the copy, called an "EnCase file," to the State's computer. Detective Avery did not testify about the exact date he began his search, but he performed an examination of the EnCase file and found images and videos pertaining to a sexual assault.

¶ 129 After Detective Avery's search, a grand jury indicted McCavitt on August 6, 2013, for the first time, on multiple counts of criminal sexual assault and aggravated criminal sexual assault. On March 19, 2014, a jury found McCavitt not guilty on all of the sexual assault charges. Once the not guilty verdict was returned in open court, McCavitt's attorney made an oral motion requesting that the trial court return items confiscated from McCavitt, including some "collector guns." The court instructed McCavitt's attorney to make his request "in the form of a motion."

¶ 130 On March 21, 2014, two days after McCavitt's acquittal, Detective James Feehan, a computer forensic examiner for the Peoria Police Department (PPD), requested a copy of the EnCase file for purposes of an internal affairs investigation of McCavitt regarding allegations of sexual assault and other possible offenses. On March 24, 2014, Detective Feehan received a copy of Detective Avery's EnCase file, searched it for images of sexual assault "as the [July 24, 2013, search] warrant had authorized," and discovered two images of child pornography.

¶ 131 Also on March 24, 2014, five days after McCavitt's acquittal and pursuant to the trial judge's instructions, his attorney filed a written motion for return of confiscated property.

¶ 132 On March 28, 2014, police arrested McCavitt and charged him with unauthorized video recording. On April 1, 2014, 13 days after McCavitt's acquittal, Feehan obtained a third warrant. Once the circuit court issued the third warrant, Feehan resumed his search and located additional images of child pornography. On

April 23, 2014, a grand jury indicted McCavitt on 10 counts of child pornography and aggravated child pornography.

¶ 133 On April 24, 2014, the circuit court entered a written order that (1) directed ISP to return all guns and weapons to McCavitt *instanter* and (2) “generally continued” McCavitt’s motion for return of confiscated property.

¶ 134 On August 15, 2014, McCavitt filed a motion to suppress evidence in the child pornography case. On October 21, 2014, the circuit court denied McCavitt’s motion to suppress evidence. On July 10, 2015, McCavitt was indicted on seven additional counts of child pornography. On July 14, 2015, a jury found McCavitt guilty of 15 of 17 counts of child pornography. On December 1, 2017, the circuit court sentenced McCavitt to five years’ imprisonment. The appellate court, with one justice dissenting, reversed McCavitt’s conviction. 2019 IL App (3d) 170830. We allowed the State’s petition for leave to appeal. Ill. S. Ct. R. 315 (eff. Oct. 1, 2019).

¶ 135 ANALYSIS

¶ 136 A. Standard of Review

¶ 137 This appeal involves a determination of McCavitt’s rights under Illinois’s constitution (Ill. Const. 1970, art. I, § 6) and statutory provisions (725 ILCS 5/108-6, 108-11 (West 2020)). When construing a constitutional provision, this court’s goal is to determine and effectuate the common understanding of the persons who adopted it—the citizens of this state—and to that end, we will consider the natural and popular meaning of the words used as well as the object to be attained or the evil to be remedied. *Walker v. McGuire*, 2015 IL 117138, ¶ 16. Where the language of a constitutional provision is unambiguous, we give it effect without resort to aids for construction (*id.*), meaning that we will not depart from the plain language of a provision by construing it so that any part is rendered meaningless or superfluous; nor will we read into a provision exceptions, limitations, or conditions that do not appear on its face or that conflict with its intent (*People v. Burge*, 2021 IL 125642, ¶ 34 (citing *People v. Perry*, 224 Ill. 2d 312, 323 (2007))). The interpretation and application of constitutional provisions presents a question of law that we review *de novo*. *Gregg v. Rauner*, 2018 IL 122802, ¶ 23 (citing *Hawthorne v. Village of Olympia Fields*, 204 Ill. 2d 243, 254-55 (2003)). We follow the same rules for

statutory interpretation that we use to construe constitutional provisions, and statutory interpretation also presents a question of law that we review *de novo*. *People v. Wise*, 2021 IL 125392, ¶ 23.

¶ 138 The ultimate issue in this case is whether the March 24, 2014, search of the State’s EnCase file with a search warrant issued 243 days earlier, on July 24, 2013, violated McCavitt’s constitutional and statutory rights. The legality of the March 24, 2014, search is a question of law we review *de novo*. *People v. Bonilla*, 2018 IL 122484, ¶ 10 (citing *People v. Caballes*, 221 Ill. 2d 282, 289 (2006)).

¶ 139 **B. McCavitt Had a Constitutional Right  
to Privacy in His Data Under Article I, Section 6,  
of the Illinois Constitution**

¶ 140 The Illinois Constitution, unlike the federal constitution, specifically codifies a person’s right to privacy in one’s person, house, papers, and possessions against unreasonable searches and seizures. Ill. Const. 1970, art. I, § 6. Privacy rights are so important to Illinois citizens that the delegates to the sixth constitutional convention codified them in Illinois’s constitution. See also *id.* § 1. “This court has observed that the Illinois Constitution goes beyond federal constitutional guarantees by expressly recognizing a zone of personal privacy, and that the protection of that privacy is stated broadly and without restrictions.” *Kunkel v. Walton*, 179 Ill. 2d 519, 537 (1997); see also Ill. Const. 1970, art. I, § 1. Therefore, article I, section 6, of the Illinois Constitution gives McCavitt a right to privacy in the data on his hard drive. Ill. Const. 1970, art. I, § 6.

¶ 141 **C. The July 24, 2013, Search Warrant  
Was Void 96 Hours After  
Its Issuance Under Section 108-6 of the Code**

¶ 142 The majority maintains that the March 24, 2014, search pursuant to the search warrant issued on July 24, 2013, was reasonable (1) because of “the intervening sexual assault prosecution” and (2) because of “the sheer volume of data in the EnCase file.” *Supra* ¶ 108.

¶ 143 The majority completely ignores the plain language of section 108-6 of the Code (725 ILCS 5/108-6 (West 2020)). See *supra* ¶¶ 105-08. Section 108-6 provides, in pertinent part, as follows: “The warrant shall be executed within 96 hours [(four days)] from the time of issuance. \*\*\* Any warrant not executed within such time shall be void and shall be returned to the court of the judge issuing the same as ‘not executed’.” 725 ILCS 5/108-6 (West 2020).

¶ 144 The plain language of section 108-6 requires warrants to be executed and searches to be conducted within 96 hours, or four days, after the date and time they were issued, or the warrant is void. See *id.* The July 24, 2013, search warrant directed the police who seized possession of McCavitt’s computer on July 17, 2013, to “search and examine in greater detail \*\*\* an LG computer tower.” There is no language in section 108-6 that tolls the running of the 96 hours (1) because of intervening prosecutions, (2) because of the volume of data in a file being searched, or (3) because of an arbitrator’s ruling or the police department’s collective bargaining agreement (*supra* ¶ 25 n.2). See 725 ILCS 5/108-6 (West 2020). There is also no evidence that the police requested that the trial judge extend the time for the police to search the data on McCavitt’s hard drive. Finally, this court may not depart from section 108-6’s plain language by reading into it exceptions, limitations, or conditions the legislature did not express. *Burge*, 2021 IL 125642, ¶ 20.

¶ 145 The United States Supreme Court provides guidance on what happens when a limitation provision in a search warrant statute expires. In *Sgro v. United States*, 287 U.S. 206, 208 (1932), a commissioner under the National Prohibition Act (Prohibition Act) issued a search warrant on July 6, 1926, pursuant to 18 U.S.C. §§ 613-616 (1926) (repealed). Section 11 of the Prohibition Act required that the “ ‘warrant must be executed and returned to the \*\*\* commissioner who issued it within ten days after its date.’ ” *Sgro*, 287 U.S. at 210 (quoting 18 U.S.C. § 621 (1926)). The Prohibition Act also provided that “ ‘after the expiration of [the 10 days] the warrant, unless executed, is void.’ ” *Id.* (quoting 18 U.S.C. § 11 (1926)). The government did not execute the warrant within 10 days of July 6, 1926. On July 27, 1926, the commissioner redated and reissued the warrant, and the government conducted the search. *Id.* at 208-09. The trial court denied the defendant’s motion to suppress evidence seized under the invalid warrant and admitted the evidence over the defendant’s objection. *Id.* at 208. The Second Circuit

Court of Appeals affirmed. *Id.* (citing *Sgro v. United States*, 54 F.2d 1083 (2d Cir. 1932)).

¶ 146 The Supreme Court noted that there was no provision in the statute that authorized the commissioner to extend the life of the warrant or to revive it. Instead, the government was required to obtain a new warrant and to follow all of the procedures under the statute. *Id.* at 211. The Supreme Court held that, because the original warrant was issued on July 6 and was not executed within 10 days, it became void and could not be redated or reissued by the commissioner. *Id.* at 210-11 (citing 18 U.S.C. § 621 (1926)).

¶ 147 On March 24, 2014, 239 days after the search warrant expired on July 28, 2013, Detective Feehan conducted a search of the EnCase file, leading to the discovery of suspected child pornography. Because the July 24, 2013, search warrant expired on July 28, 2013, and therefore was void (see *id.* at 208-09), the search warrant did not confer any rights on the State or Detective Feehan to conduct the March 24, 2014, search of McCavitt's data. The 243-day delay in searching McCavitt's data was unreasonable and violated McCavitt's constitutional and statutory rights. Ill. Const. 1970, art. I, § 6; 725 ILCS 5/108-6 (West 2020).

¶ 148 The July 24, 2013, search warrant expired on July 28, 2013, and was void (see *Sgro*, 287 U.S. at 208-09), and the search the police conducted on March 24, 2014, 239 days after the search warrant expired, violated section 108-6 (see 725 ILCS 5/108-6 (West 2020); see also *Sgro*, 287 U.S. at 212). Moreover, any evidence that Detective Feehan may have discovered in plain view on March 24, 2014, pursuant to the void July 24, 2013, search warrant was the fruit of the illegal search and must be suppressed. See *Wong Sun v. United States*, 371 U.S. 471, 485-88 (1963) (holding that evidence seized during an unlawful search cannot be used as proof against the victim of the search when the unlawful conduct of the police cannot be purged from the primary taint). Therefore, following *Sgro*, I submit that the July 24, 2013, search warrant became void on July 28, 2013, and that, without a new warrant, no search could take place after that date and any evidence seized was the fruit of the illegal search. *Id.*

¶ 149

D. McCavitt Had a Right to Have  
His Hard Drive Returned Under Section 108-11

¶ 150

The majority takes the position that section 108-11 “contemplates a motion and a hearing before an order is entered disposing of seized items.” *Supra* ¶ 82. I submit that the majority is ignoring the plain language of the statute and, therefore, the trial court’s failure to order the return of McCavitt’s property, *instanter*, cannot be justified by McCavitt’s failure to file a written motion. See 725 ILCS 5/108-11 (West 2020).

¶ 151

Section 108-11 of the Code provides: “The court before which the instruments, articles or things are returned shall enter an order providing for their custody pending further proceedings.” 725 ILCS 5/108-11 (West 2020). There is nothing in the plain language of section 108-11 to support the majority’s position that the statute has a written motion or hearing requirement. See *id.* The majority has read conditions into the statute—a requirement for a motion and a hearing—that are not contained in the plain language of the statute. See *id.* The majority violates this court’s well-established rules of statutory construction that the court will not depart from the plain statutory language by reading in exceptions, limitations, or conditions not expressed by the legislature. *People v. Wise*, 2021 IL 125392, ¶ 23. The majority ignored the language in section 108-11 of the Code when it found that McCavitt failed to file a motion or request a hearing for return of his computer and the data on his hard drive. *Supra* ¶ 82.

¶ 152

When the State seizes property pursuant to a valid warrant (the July 24, 2013, search warrant expired on July 28, 2013, and was void), the custody and disposition of the seized property is controlled by section 108-11 of the Code. See *People ex rel. Carey v. Covelli*, 61 Ill. 2d 394 (1975); 725 ILCS 5/108-11 (West 2020). This court has construed section 108-11 to be the applicable statute when a person seeks the return of property seized by the State. See *Covelli*, 61 Ill. 2d 394. In *Covelli*, the plaintiffs sought the return of their deceased father’s property that police seized pursuant to a search warrant to discover the identity of the person who murdered their father. *Id.* at 398. The plaintiffs argued that section 114-12(a) of the Code (Ill. Rev. Stat. 1973, ch. 38, ¶ 114-12) did not provide a remedy for the return of their father’s property because there were no “defendants” in the case, as no one had been charged with the murder. *Covelli*, 61 Ill. 2d at 402. This court rejected the

plaintiffs’ argument and pointed out that the plaintiffs had “failed to consider article 108 of the Code.” *Id.* This court held that section 108-11 of the Code provided protection to the plaintiffs’ interests in their “property and privacy.” *Id.* at 403.

¶ 153 Section 108-11 gave the trial court, upon McCavitt’s March 19, 2014, acquittal with the entry of the not guilty jury verdict, the authority to order the return of McCavitt’s property *instanter* since the statute did not require McCavitt to file a motion or the judge to hold a hearing. 725 ILCS 5/108-11 (West 2020). It should be noted that, after a hearing on McCavitt’s written motion, the trial judge ordered the return of McCavitt’s guns but continued the remainder of the motion. The trial judge abused his discretion by failing to order a return of the EnCase file upon McCavitt’s acquittal and his attorney’s oral motion on March 19, 2014, because, without a motion or hearing requirement, section 108-11 of the Code gave the trial court authority, *sua sponte*, to enter an order directing the State to return McCavitt’s seized property. See *id.*

¶ 154 1. McCavitt’s Right to His Computer Data  
Was Never Lost So It Did Not Need to Be Restored

¶ 155 The majority maintains, without citation of authority, that McCavitt’s acquittal only partially restored his expectation of privacy in his data. *Supra* ¶ 72. The majority takes the position that, after the March 19, 2014, acquittal, the July 24, 2013, search warrant “still authorized a search for evidence of unauthorized video recording[s].” *Supra* ¶ 106. The majority cites the double jeopardy provision in support of its position that upon McCavitt’s acquittal he only “regained a reasonable expectation that the police would not search his computer for evidence of the offenses of which he was acquitted [on March 19, 2014.]” *Supra* ¶ 76.

¶ 156 I disagree. The double jeopardy provision only prevents McCavitt from being tried a second time for the criminal sexual assault offenses for which he was acquitted. See Ill. Const. 1970, art. I, § 10 (“No person shall be \*\*\* twice put in jeopardy for the same offense.”). The double jeopardy provision did not determine whether McCavitt’s article I, section 6, right to privacy in his computer data was fully restored upon his acquittal.

¶ 157 Illinois’s constitution and statutes codify a right to vote, serve on a jury, and hold public office. See Ill. Const. 1970, art. III, § 1; *id.* art. XIII, § 1; 705 ILCS 305/1, 2 (West 2020); see *Hoskins v. Walker*, 57 Ill. 2d 503, 508-09 (1974) (finding the right to be a candidate for office is not absolute and limitations may be imposed by the legislature). Upon conviction of a felony, Illinois’s constitution and statutes provide that a person shall lose the rights to vote, to serve on a jury, and to hold public office. See Ill. Const. 1970, art. III, § 2; *id.* art. XIII, § 1; 705 ILCS 305/2(a)(3) (West 2020). Illinois’s constitution and statutes also provide that certain rights that are lost because of a conviction of a felony are immediately restored upon completion of the sentence. Ill. Const. 1970, art. III, § 2; 730 ILCS 5/5-5-5(a), (b), (c) (West 2020); 705 ILCS 305/2(a)(3) (West 2020) (“Jurors must be: \*\*\* [f]ree from all legal exception”). Illinois statutes also provide that the rights to vote, to serve on a jury, and to hold public office are automatically restored no later than upon the completion of any sentence for a felony conviction. 705 ILCS 305/2(a)(3) (West 2020); 730 ILCS 5/5-5-5(a), (b), (c) (West 2020). A conviction does not result in the loss of any “civil rights” except as provided by section 5-5-5 of the Unified Code of Corrections (730 ILCS 5/5-5-5 (West 2020)) or sections 29-6 and 29-10 of the Election Code (10 ILCS 5/29-6, 29-10 (West 2020)).

¶ 158 It should be noted that neither Illinois’s constitution nor its statutes provide for a loss of the right to privacy at any time. See Ill. Const. 1970; 730 ILCS 5/5-5-5 (West 2020). I submit that the right to privacy in one’s property, like the rights to vote, serve on a jury, and hold public office, can only be lost, if lost at all, upon conviction of a felony. See Ill. Const. 1970, art. III, § 2; *id.* art. XIII, § 1; 705 ILCS 305/2(a)(3) (West 2020).

¶ 159 Here, McCavitt was only charged with criminal offenses for which he was presumed innocent. See *People v. Robinson*, 167 Ill. 2d 53, 74 (1995). Because McCavitt was acquitted and had not been convicted of a felony on March 19, 2014, he never lost his right to his property and was not required by section 108-11 to take any action, including filing a motion, to have the trial judge return his property. 725 ILCS 5/108-11 (West 2020); see also Ill. Const. 1970, art. I, § 6; *id.* art. I, § 13; *id.* art. XIII, § 1; 705 ILCS 305/2(a)(3) (West 2020); 730 ILCS 5/5-5-5(a), (b), (c) (West 2020). Therefore, since McCavitt’s article I, section 6, right to his property was never lost, and since the two images of child pornography were found by Detective Feehan on March 24, 2014, five days after McCavitt’s acquittal, his



that was void because it was issued 243 days before the search was conducted by the police. *Id.* Second, *Hughes* is also inapposite because there was no Michigan statute like section 108-6 of the Code that placed a 96-hour limit on the execution of a search warrant by the police. See *id.* at 106; Mich. Comp. Laws § 780.651 (2014). Third, *Hughes* is inapposite because the defendant in *Hughes* was not acquitted of certain charges delineated in the warrant. *Hughes*, 958 N.W.2d at 104-05. Therefore, because Detective Feehan could not conduct a search for data within the scope of the void July 24, 2013, search warrant, *Hughes* provides no support for the majority's position.

¶ 165

#### CONCLUSION

¶ 166

McCavitt had a constitutional right to the control and possession of his data until the issuance of the July 17, 2013, and July 24, 2013, search warrants. *Riley*, 573 U.S. at 386. Upon the issuance of the July 17, 2013, and July 24, 2013, search warrants, McCavitt's right to his property was temporarily suspended but was never lost because he had not been convicted of a felony on March 24, 2014, and the warrants gave the police 96 hours to search the data on his hard drive. In light of the fact that the July 24, 2013, search warrant became void on July 28, 2013, McCavitt's March 19, 2014, acquittal immediately restored his right to the immediate return of the data in the State's EnCase file. The evidence the police discovered after July 28, 2013, was the fruit of an illegal search with a void search warrant and should not have been admitted into evidence against McCavitt. The legislature should amend section 108-11 of the Code and make it clear that, after an acquittal, a citizen's property (1) that is seized pursuant to a valid search warrant and (2) that is not contraband or obscene must be returned *instanter*. Therefore, I respectfully dissent, and I would affirm the appellate court's judgment and remand this case to the circuit court with directions to exclude all evidence that was discovered by the police during the illegal search conducted by the police after July 28, 2013.

RECEIVED  
03-04-2021  
CLERK OF WISCONSIN  
SUPREME COURT

IN THE SUPREME COURT OF WISCONSIN

---

STATE OF WISCONSIN

Plaintiff-Respondent,

Appeal No.

2019-AP-1404-CR

v.

GEORGE STEVEN BURCH,

Defendant-Appellant.

---

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION FOUNDATION,  
AMERICAN CIVIL LIBERTIES UNION OF WISCONSIN FOUNDATION,  
ELECTRONIC FRONTIER FOUNDATION, AND ELECTRONIC PRIVACY  
INFORMATION CENTER

---

Laurence J. Dupuis (WBN 1029261)  
American Civil Liberties Union of  
Wisconsin Foundation  
207 E. Buffalo Street, Suite 325  
Milwaukee, WI 53202  
Telephone: (414) 272-4032, ext. 212  
Email: ldupuis@aclu-wi.org

Jennifer Granick, admitted *pro hac vice*  
American Civil Liberties  
Union Foundation  
39 Drumm Street  
San Francisco, CA 94111  
Telephone: (415) 343-0758  
Email: jgranick@aclu.org

Jennifer Lynch, admitted *pro hac vice*  
Electronic Frontier Foundation  
815 Eddy Street  
San Francisco, CA 94109  
Telephone: (415) 435-9333  
Email: jlynch@eff.org

## TABLE OF CONTENTS

STATEMENT OF INTEREST OF AMICI .....	1
INTRODUCTION .....	3
ARGUMENT .....	4
I. CELL PHONES GENERATE, STORE, AND PROVIDE ACCESS TO VAST QUANTITIES OF SENSITIVE PERSONAL INFORMATION THAT REQUIRE HEIGHTENED CONSTITUTIONAL PROTECTIONS AGAINST WARRANTLESS EXTRACTION, ANALYSIS, AND STORAGE.....	4
A. Cell phone searches raise significant privacy concerns because they provide access to vast amounts of personal information. ....	4
B. Law enforcement increasingly extracts, analyzes, and stores the entire contents of cell phones using advanced forensic tools—often without a warrant.....	6
II. CONSENT-BASED SEARCHES OF DIGITAL DATA MUST BE NARROWLY SCOPED IN CATEGORY AND PURPOSE TO THE OWNER’S EXPLICIT PERMISSION.....	9
A. A reasonable person would understand consent to search their cell phone as limited to common-sense categories of relevant information, such as the text messages in this case, and not to include a full forensic download and analysis.....	10
B. Consent searches are also limited in scope to the purposes for which a reasonable person would understand their data is being examined.....	13
C. Limitations on consent are particularly important because consent searches of cell phones raise unique concerns about law enforcement coercion.....	13
D. Consent forms deserve little weight because they often fail to provide people facing an investigation sufficient information about their rights or about what a search means.....	14
III. THE RETENTION OF BURCH’S CELL PHONE DATA VIOLATED THE FOURTH AMENDMENT.....	16
A. Copying Burch’s digital data constituted a seizure under the Fourth Amendment.....	16
B. It was unreasonable for the State to retain everything on Burch’s phone.....	17

C. The Fourth Amendment requires that law enforcement purge or return  
unreasonably seized digital data..... 19

IV. THE BROWN COUNTY SHERIFF OFFICE’S SUBSEQUENT SEARCH OF  
BURCH’S DATA VIOLATED THE FOURTH AMENDMENT. .... 21

CONCLUSION..... 22

CERTIFICATION AS TO FORM AND LENGTH..... 23

CERTIFICATE OF COMPLIANCE WITH WIS. STAT. § 809.19(12)..... 24

## TABLE OF AUTHORITIES

### CASES

<i>Andresen v. Maryland</i> , 427 U.S. 463 (1976) .....	19
<i>Arizona v. Gant</i> , 556 U.S. 332 (2009) .....	3
<i>Belleau v. Wall</i> , 811 F.3d 929 (7th Cir. 2016) .....	2
<i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018).....	1, 6
<i>Coolidge v. New Hampshire</i> , 403 U.S. 443 (1971) .....	3
<i>Florida v. Jimeno</i> , 500 U.S. 248 (1991) .....	10, 13
<i>In re Search of Black iPhone 4</i> , 27 F. Supp. 3d 74 (D.D.C. 2014).....	20
<i>In re Search of Info. Associated with the Facebook Acct. Identified by the Username Aaron.Alexis That Is Stored at Premises Controlled by Facebook, Inc.</i> , 21 F. Supp. 3d 1 (D.D.C. 2013).....	20
<i>In the Matter of the Search of Premises Known as a Nextel Cellular Tel.</i> , No. 14-MJ-8005-DJW, 2014 WL 2898262 (D. Kan. June 26, 2014) .....	20
<i>Kentucky v. King</i> , 563 U.S. 452 (2011) .....	19
<i>Matter of Search of ODYS LOOX Plus Tablet Serial No. 4707213703415 in Custody of United States Postal Inspection Serv., 1400 New York Ave NW, Washington, DC</i> ,	

28 F. Supp. 3d 40 (D.D.C. 2014).....	20
<i>Matter of the Search of Apple iPhone, IMEI 013888003738427,</i> 31 F. Supp. 3d 159 (D.D.C. 2014).....	20
<i>Payton v. New York,</i> 445 U.S. 573 (1980) .....	9
<i>People v. Hughes,</i> No. 158652, 2020 WL 8022850 (Mich. 2020) .....	2
<i>People v. Thompson,</i> 28 N.Y.S.3d 237 (N.Y. Sup. Ct. 2016).....	17
<i>Riley v. California,</i> 573 U.S. 373 (2014) .....	passim
<i>Schneckloth v. Bustamonte,</i> 412 U.S. 218 (1973) .....	10
<i>State v. Burch,</i> No. 2019AP1404-CR (Wis. Ct. App. Oct. 20, 2020) .....	12, 15
<i>State v. Mansor,</i> 421 P.3d 323 (Or. 2018) .....	20
<i>State v. Matejka,</i> 2001 WI 5, 241 Wis. 2d 52, 621 N.W.2d 891 .....	11
<i>State v. Phillips,</i> 218 Wis. 2d 180, 577 N.W.2d 794 (1998) .....	10
<i>State v. Randall,</i> 2019 WI 80, 387 Wis. 2d 744, 930 N.W.2d 223 .....	9, 22

<i>State v. Sveum</i> , 2010 WI 92, 328 Wis. 2d 369, 787 N.W.2d 317 .....	2
<i>Terry v. Ohio</i> , 392 U.S. 1 (1968) .....	17
<i>United States v. Blocker</i> , 104 F.3d 720 (5th Cir. 1997) .....	13
<i>United States v. Bosse</i> , 898 F.2d 113 (9th Cir.1990) .....	13
<i>United States v. Comprehensive Drug Testing, Inc.</i> , 621 F.3d 1162 (9th Cir. 2010) .....	16, 17, 18, 21
<i>United States v. Galpin</i> , 720 F.3d 436 (2d Cir. 2013) .....	18
<i>United States v. Ganas</i> , 824 F.3d 199 (2d Cir. 2016) .....	2, 16, 20, 21
<i>United States v. Hulscher</i> , No. 4:16-CR-40070-01-KES, 2017 WL 657436 (D.S.D. Feb. 17, 2017) .....	21
<i>United States v. Jacobsen</i> , 466 U.S. 109 (1984) .....	16, 17, 18
<i>United States v. Jones</i> , 565 U.S. 400 (2012) .....	1, 3
<i>United States v. Karo</i> , 468 U.S. 705 (1984) .....	16
<i>United States v. Metter</i> , 860 F. Supp. 2d 205 (E.D.N.Y. 2012) .....	19

<i>United States v. Miller</i> , 982 F.3d 412 (6th Cir. 2020) .....	1
<i>United States v. Morton</i> , 984 F.3d 421 (5th Cir. 2021) .....	11
<i>United States v. Patrick</i> , 842 F.3d 540 (7th Cir. 2016) .....	2
<i>United States v. Place</i> , 462 U.S. 696, 710 (1983) .....	17
<i>United States v. Sedaghaty</i> , 728 F.3d 885 (9th Cir. 2013) .....	21
<i>United States v. Tamura</i> , 694 F.2d 591 (9th Cir. 1982) .....	18
<i>United States v. Washington</i> , 490 F.3d 765 (9th Cir. 2007) .....	14
<i>United States v. Werdene</i> , 883 F.3d 204 (3d Cir. 2018) .....	16
<i>United States v. Wey</i> , 256 F. Supp. 3d 355 (S.D.N.Y. 2017) .....	21
<i>Walter v. United States</i> , 447 U.S. 649 (1980) .....	9, 11

## **OTHER AUTHORITIES**

Alan Butler, <i>Get a Warrant: The S. Ct. 's New Course for Digit. Privacy Rights After Riley v. California</i> , 10 Duke J. Const. L. & Pub. Pol'y 83 (2014).....	5
---	---

App Annie, <i>State of Mobile 2021</i> (2020), <a href="https://www.appannie.com/en/go/state-of-mobile-2021/">https://www.appannie.com/en/go/state-of-mobile-2021/</a> .....	6
Apple, <i>Compare iPhone Models</i> , <a href="https://perma.cc/A7G9-AJQX">https://perma.cc/A7G9-AJQX</a> .....	5
Apple, <i>iCloud</i> (2021), <a href="https://perma.cc/5UMQ-NV3K">https://perma.cc/5UMQ-NV3K</a> .....	5
Benjamin D. Douglas et al., <i>Some Rschs. Wear Yellow Pants, but Even Fewer Participants Read Consent Forms: Exploring and Improving Consent Form Reading in Human Subjects Rsch.</i> , 26 Psych. Methods 61 (2021) .....	15
Devon W. Carbado, <i>(E)Racing the Fourth Amend.</i> , 100 Mich. L. Rev. 946 (2002) .....	14
iClick, <i>How Big is a Gig?</i> (2013), <a href="https://www.iclick.com/pdf/02_howbigisagig_infographic.pdf">https://www.iclick.com/pdf/02_howbigisagig_infographic.pdf</a> .....	5
J.D. Biersdorfer, <i>Getting Alerts from a Digital Pillbox</i> , N.Y. Times (June 5, 2017), <a href="https://perma.cc/M4DR-DABR">https://perma.cc/M4DR-DABR</a> .....	14
Janice Nadler, <i>No Need to Shout: Bus Sweeps and the Psych. of Coercion</i> , 2002 Sup. Ct. Rev. 153 (2002) .....	14
Laurent Sacharoff, <i>The Fourth Amend. Inventory as a Check on Digit. Searches</i> , 105 Iowa L. Rev. 1643 (2020) .....	19
Marcy Strauss, <i>Reconstructing Consent</i> , 92 J. Crim. L. & Criminology 211 (2002) .....	13
Nancy Leong & Kira Suyeishi, <i>Consent Forms and Consent Formalism</i> , 2013 Wis. L. Rev. 751 (2013) .....	15
Orin S. Kerr, <i>Executing Warrants for Digit. Evid.: The Case for Use Restrictions on Nonresponsive Data</i> ,	

48 Tex. Tech. L. Rev. 1 (2015) .....	21
Pew Rsch. Ctr., <i>Mobile Fact Sheet</i> (June 12, 2019), <a href="https://www.pewresearch.org/internet/fact-sheet/mobile/">https://www.pewresearch.org/internet/fact-sheet/mobile/</a> .....	5
Ric Simmons, <i>Not “Voluntary” but Still Reasonable: A New Paradigm for Understanding the Consent Searches Doctrine</i> , 80 Ind. L. J. 773 (2005) .....	8
Samsung, <i>Galaxy S10+ 1TB (Unlocked)</i> , <a href="https://perma.cc/8BJ4-EP9W">https://perma.cc/8BJ4-EP9W</a> . .....	5
Upturn, <i>Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones</i> (Oct. 2020), <a href="https://perma.cc/7DCK-PGMQ">https://perma.cc/7DCK-PGMQ</a> .....	7, 8, 12, 15

## STATEMENT OF INTEREST OF AMICI

The American Civil Liberties Union (“ACLU”) is a nationwide, nonprofit, nonpartisan organization dedicated to defending the principles embodied in the Federal Constitution and our nation’s civil rights laws. The ACLU of Wisconsin Foundation is the local affiliate of the ACLU. The ACLU and the ACLU of Wisconsin have frequently appeared before courts—including this one—throughout the country in Fourth Amendment cases, both as direct counsel and as amici curiae.

The Electronic Frontier Foundation (“EFF”) is a member-supported, nonprofit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for nearly thirty years. With roughly 35,000 active donors, including donors in Wisconsin, EFF represents technology users’ interests in court cases and broader policy debates. EFF regularly participates both as direct counsel and as amicus in the Supreme Court, the Seventh Circuit Court of Appeals, this Court, and other state and federal courts in cases addressing the Fourth Amendment and its application to new technologies.

The Electronic Privacy Information Center (“EPIC”) is a public-interest research center in Washington, D.C. established to focus public attention on emerging privacy and civil liberties issues in the information age. EPIC participates as amicus curiae before courts across the country in cases involving constitutional rights and emerging technologies.

Amici have, alone or together, appeared as either counsel or amicus in the following cases: *Carpenter v. United States*, 138 S. Ct. 2206 (2018); *Riley v. California*, 573 U.S. 373 (2014); *United States v. Jones*, 565 U.S. 400 (2012); *United States v. Miller*, 982 F.3d 412 (6th Cir. 2020), *petition for cert. filed*, (U.S. Feb. 25, 2021) (No. 20-1202) (Google’s use of a proprietary algorithm to automatically search user data and refer to law enforcement); *State v. Sveum*, 2010 WI 92, 328 Wis. 2d 369, 787 N.W.2d 317 (warrantless GPS tracking of vehicles); *Belleau v. Wall*, 811 F.3d 929 (7th Cir. 2016)

(GPS bracelets); *United States v. Ganius*, 824 F.3d 199 (2d Cir. 2016) (en banc); *United States v. Patrick*, 842 F.3d 540 (7th Cir. 2016), *reh 'g denied* (7th Cir. May 9, 2017) (cell-site simulators); *People v. Hughes*, No. 158652, 2020 WL 8022850 (Mich. 2020) (police searched cell phone data obtained in one investigation for evidence of a different crime).

Given this expertise, amici's participation may be helpful to this Court. The Court granted leave to file this brief on February 9, 2021. Order Granting Amici's Mot. to File a Non-Party Br.<sup>1</sup>

---

<sup>1</sup> Amici wish to thank Rachel Maremont, a student at New York University School of Law, and Melodi Dincer, a legal fellow at EPIC, for their contributions to this brief.

## INTRODUCTION

The “central concern underlying the Fourth Amendment” is to avoid “giving police officers unbridled discretion to rummage at will among a person’s private effects.” *Arizona v. Gant*, 556 U.S. 332, 345 (2009). Yet, the State’s position in this case—that it is authorized to indefinitely retain all of Burch’s cell phone data and search it for any reason—opens the door to just such “general, exploratory rummaging” as the “‘general warrant’ abhorred by the colonists.” *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). Under the State’s proposed rule, no one—including suspects, witnesses, and victims—who consents to a search of their digital device in the context of one investigation could prevent law enforcement from storing a copy of their *entire* device in a database and “min[ing] [it] for information years into the future.” *United States v. Jones*, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). Such a rule would enable the State to rummage at will among a person’s most personal and private information whenever it wanted, for as long as it wanted. *See Riley v. California*, 573 U.S. 373, 399 (2014) (requiring greater protections for searches of digital data because “[t]he sources of potential pertinent information are virtually unlimited”). The Constitution does not grant the police such power.

For the reasons set forth below, amici answer this Court’s questions presented as follows:

1. A reasonable person would consider the scope of consent to search a cell phone to be limited by the discussion with police identifying specific categories of data, and would believe that a download of “the information” referred to the categories of information discussed, not to a forensic download and search of the phone’s entire contents.
2. Vague consent forms such as the one in this case cannot override more explicit oral statements and assurances about the scope of consent.
3. After police downloaded information from the cell phone, they could have retained and searched only the information Burch consented to share—his text messages from the night before the hit-and-run. *See* R. 234:9–10, App’x at 108–09. Any search of

that data also had to be limited to the context in which consent was given—the investigation of the hit-and-run.

4. The ongoing retention of information the police were permitted to access became unreasonable once police determined Burch was no longer a suspect in the hit-and-run investigation.

5. That Burch was no longer a suspect in the original investigation is a strong indication that continued retention of his data was unlawful.

6. Police first had an obligation to immediately return to Burch material outside the scope of consent, because it should never have been seized. Second, after officers completed their search by creating a report containing communications potentially relevant to the hit-and-run investigation, the remainder of Burch’s data, which was non-responsive, should have been returned. Finally, when police determined that Burch was no longer a suspect, all his information should have been returned.

## ARGUMENT

### **I. CELL PHONES GENERATE, STORE, AND PROVIDE ACCESS TO VAST QUANTITIES OF SENSITIVE PERSONAL INFORMATION THAT REQUIRE HEIGHTENED CONSTITUTIONAL PROTECTIONS AGAINST WARRANTLESS EXTRACTION, ANALYSIS, AND STORAGE.**

Modern cell phones contain a wealth of sensitive information that would never have been accessible to law enforcement before. Today, government agencies have advanced forensic tools that can extract and analyze all of the data stored on a cell phone, including data that the user might not even know exists. When law enforcement obtains and analyzes an individual’s cell phone data, it invades that individual’s expectation of privacy protected by the Fourth Amendment, and it must obtain a warrant or an exception to the warrant requirement must apply.

#### **A. Cell phone searches raise significant privacy concerns because they provide access to vast amounts of personal information.**

A smartphone is a palm-sized portal into an individual’s personal life. Smartphones “place vast quantities of personal information literally in the hands of

individuals.” *Riley*, 573 U.S. at 386. The more than eighty percent<sup>2</sup> of Americans who own smartphones “keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate.” *Riley*, 573 U.S. at 395.

In *Riley*, the U.S. Supreme Court recognized that cell phone searches “implicate privacy concerns far beyond those implicated” by the search of any other object and thus require heightened constitutional protections. *Id.* at 393. This is partly because “cell phones have become [a] pervasive and insistent . . . part of daily life”—so much so that they appear almost “as an important feature of human anatomy.” *Id.* at 385; *see also* Alan Butler, *Get a Warrant: The S. Ct.’s New Course for Digit. Privacy Rights After Riley v. California*, 10 Duke J. Const. L. & Pub. Pol’y 83, 89–91 (2014).

Cell phone searches involve a quantitatively different privacy intrusion as compared to searches of physical items because of cell phones’ “immense storage capacity.” *Riley*, 573 U.S. at 385. In 2014, when the Supreme Court decided *Riley*, the top-selling smartphone could store sixteen gigabytes of data. *Id.* at 394.<sup>3</sup> The minimum storage on Apple’s current line of iPhones is sixty-four gigabytes.<sup>4</sup> Some Android models offer one terabyte of storage, roughly sixty-four times more than a *Riley*-era phone.<sup>5</sup> And off-device cloud storage services expand capacity even further.<sup>6</sup> Storage capacities increase every year, as does the sheer volume of personal data stored on—and accessible from—cell phones.

Cell phones are also qualitatively different from other objects because they “collect[] in one place many distinct types of information—an address, a note, a

---

<sup>2</sup> Pew Rsch. Ctr., *Mobile Fact Sheet* (June 12, 2019), <https://www.pewresearch.org/internet/fact-sheet/mobile/>.

<sup>3</sup> Sixteen gigabytes equals about 3,680 songs, 8,672 digital copies of *War and Peace*, 9,520 digital photos, or eight feature-length movies. *See* iClick, *How Big is a Gig?* (2013), [https://www.iclick.com/pdf/02\\_howbigisagig\\_infographic.pdf](https://www.iclick.com/pdf/02_howbigisagig_infographic.pdf).

<sup>4</sup> Apple, *Compare iPhone Models*, <https://perma.cc/A7G9-AJQX> (last visited Mar. 3, 2021).

<sup>5</sup> Samsung, *Galaxy S10+ 1TB (Unlocked)*, <https://perma.cc/8BJ4-EP9W> (last visited Mar. 3, 2021).

<sup>6</sup> Apple, *iCloud* (2021), <https://perma.cc/5UMQ-NV3K> (last visited Mar. 3, 2021) (providing up to 2TB of remote storage).

prescription, a bank statement, a video—that reveal much more in combination than any isolated record.” *Riley*, 573 U.S. at 394. Along with more traditional data like text messages, phone calls, and emails, the proliferation of smartphone apps<sup>7</sup> for social media, health and activity, dating, video streaming, mobile shopping, banking, and password storage have created novel types of records that can “reveal an individual’s private interests or concerns.” *Riley*, 573 U.S. at 395. Location information in particular is “detailed, encyclopedic, and effortlessly compiled” by most apps whenever a “cell phone faithfully follows its owner . . . into private residences, doctor’s offices, political headquarters, and other potentially revealing locales.” *Carpenter v. United States*, 138 S. Ct. 2206, 2216, 2218 (2018).

**B. Law enforcement increasingly extracts, analyzes, and stores the entire contents of cell phones using advanced forensic tools—often without a warrant.**

In recent years, law enforcement agencies across the country have acquired powerful new tools, like the technology used in this case, to conduct detailed forensic searches of cell phones. These forensic search techniques are problematic because of how much personal information the searches can reveal when all of the data from a phone is extracted, organized, and categorized in unexpected ways, stored indefinitely, combined with other data, and used to generate leads in cases completely unrelated to the original search. There is simply no physical analog to the type of detailed information that law enforcement can obtain from a forensic cell phone search.

Mobile device forensic tools (“MDFTs”) enable law enforcement to first extract and then analyze a complete copy of a cellphone’s contents. Upturn, *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones* (Oct. 2020),

---

<sup>7</sup> See App Annie, *State of Mobile 2021* (2020), <https://www.appannie.com/en/go/state-of-mobile-2021/> (gathering the most popular apps of 2020).

<https://perma.cc/7DCK-PGMQ> [hereinafter Upturn Report].<sup>8</sup> MDFTs extract “the maximum amount of information possible” from a phone, including a user’s contacts, call logs, text conversations, photos, videos, saved passwords, GPS location records, phone usage records, online account information, and app data. *Id.* at 10, 16. MDFTs can access data stored remotely in the cloud and even data the user previously deleted. *Id.* at 16–17, 21–23. MDFTs can also use login credentials stored on a phone to extract data from apps and services that are otherwise password-protected. *Id.* at 17–20.

MDFTs enable law enforcement to organize and draw connections in extracted data. They can aggregate data from different apps and sort it by GPS location, file type, or the time and date of creation, enabling police to view the data in ways a phone user cannot, and to gain insights that would be impossible if the data were siloed by application. *Id.* at 12. Police can use a MDFT’s data-sorting capability to make sense of reams of data and tell a particular story about a person, including by revealing where they were (and what they were doing), when, with whom, and even why.

An individual who gives police permission to take a quick look at their phone would be astounded at what the officers can learn when they use a MDFT, as the officers did in this case. Police can tell where and when somebody went to their place of worship. They can learn that a person has several joint bank accounts with a person of the same gender who is also tagged in hundreds of their photos. Police can also see that a person was at a recent protest where law enforcement made mass arrests, can read the person’s deleted texts, and can download deleted photos from the event to analyze the faces of others present. They can even download the person’s contacts from multiple apps, combine the data with contacts from other phones, and reveal the person’s place in an extended network of individuals.

---

<sup>8</sup> Upturn is a 501(c)(3) organization that works in partnership with many of the nation’s leading civil rights and public interest organizations to promote equity and justice in the design, governance, and use of digital technology.

Today, law enforcement agencies of all sizes in all fifty states and the District of Columbia have access to these powerful data extraction and analysis tools and use them frequently, placing “[e]very American [ ] at risk of having their phone forensically searched by law enforcement.” *Id.* at 32. At least 2,000 law enforcement agencies have purchased MDFTs, while agencies without their own MDFTs often access them through partnerships with MDFT-equipped departments or through federal forensic laboratories. *Id.* at 32, 35, 39. Many police departments readily admit that they consider MDFTs a standard investigatory tool and use them daily. *Id.* at 47. At least 50,000 cell phone extractions took place between 2015 and 2019 among the forty-four agencies that reported statistics to Upturn. *Id.* at 41. This is a “*severe undercount*” of the national number, as the vast majority of the agencies that currently use MDFTs did not respond to Upturn’s inquiries or did not track MDFT use statistics for the full period covered in the report. *Id.*

Despite the outcome of *Riley*, 573 U.S. at 386, many MDFT searches occur without warrants. Upturn’s recent report shows that police frequently conduct detailed, warrantless forensic searches of cell phone data based on users’ purported consent. Upturn Report at 46–47.<sup>9</sup> Some examples are striking: of the 1,583 cell phones on which the Harris County, Texas Sheriff’s Office performed extractive searches from August 2015 to July 2019, 53 percent were consent searches or searches of “abandoned/deceased” phones. *Id.* at 46. Of the 497 cell phone extractions performed in Anoka County, Minnesota between 2017 to May 2019, 38 percent were consent searches. *Id.* at 47.

Once law enforcement extracts cell phone data, it has the technological capability to store the data forever and search it at will. The agency thus possesses massive amounts of information about a person that, unless subject to legal limitations, could be retained

---

<sup>9</sup> Consent has become an increasingly common justification for searches of physical evidence as well. See, e.g., Ric Simmons, *Not “Voluntary” but Still Reasonable: A New Paradigm for Understanding the Consent Searches Doctrine*, 80 Ind. L. J. 773 (2005) (more than 90 percent of warrantless searches are accomplished through the use of consent).

indefinitely and searched at a later date. This is an unreasonable power for police to wield without strict constitutional review and independent judicial oversight.

**II. CONSENT-BASED SEARCHES OF DIGITAL DATA MUST BE NARROWLY SCOPED IN CATEGORY AND PURPOSE TO THE OWNER'S EXPLICIT PERMISSION.**

Both consent searches and warrant-based searches are “limited by the terms of [their] authorization.” *Walter v. United States*, 447 U.S. 649, 656 (1980). This requirement helps avoid the indiscriminate searches and seizures that were the “immediate evils” motivating adoption of the Fourth Amendment. *Id.* at 657 (citing *Payton v. New York*, 445 U.S. 573, 583 (1980)). Further, as this Court has held, searches and seizures conducted on the basis of consent are reasonable only if conducted within the scope of the consent. *See State v. Randall*, 2019 WI 80, ¶ 10, 387 Wis. 2d 744, 930 N.W.2d 223. Given that cell phone searches can reveal voluminous amounts of people’s most sensitive information through advanced forensic tools and the enormous privacy implications of allowing broad law enforcement access to this data, courts should narrowly interpret the scope of consent when a cell phone search is in question.

A reasonable person in Burch’s position would consider their consent to search a cell phone to extend only to categories of data explicitly discussed with law enforcement in lay terms—not a forensic search of the phone’s entire contents. A reasonable person would not expect a vague consent form to override previously limited verbal consent. Moreover, just as a warrant limits the scope of a search to the crime supported by probable cause, a reasonable person would also consider their consent to extend only to a search for evidence of the crime under investigation, and not to indefinite storage and use of their data to develop leads for investigations of other crimes.

Given the breadth and sensitivity of data on cell phones—the exact kind of information the Supreme Court said required heightened constitutional protections in *Riley*, 573 U.S. 373—the risks of a consent search to the device owner are severe. Consent searches are especially problematic because they are conducted without judicial authorization or oversight. Allowing law enforcement’s unfettered access to Burch’s

complete cell phone data in this case and the subsequent searches that police conducted months after that data was collected, for purposes never contemplated at the time of consent, would mean that the government may invade any individual's privacy—including victims' and witnesses'—in a similar manner without due justification in future cases.

**A. A reasonable person would understand consent to search their cell phone as limited to common-sense categories of relevant information, such as the text messages in this case, and not to include a full forensic download and analysis.**

A reasonable person would not believe that giving consent to search the text messages on their cell phone, or even to “the information” stored there, would mean they were giving the police permission to perform a complete search of the phone or to use MDFTs to extract and store all of the phone's data. Consent searches have always been limited by the scope of the permission granted. *Florida v. Jimeno*, 500 U.S. 248, 252 (1991). Especially given the unique nature of digital data and the powerful tools law enforcement agencies now possess, it is objectively reasonable to define consent to search a cell phone as including only a limited, manual search, at least in the absence of clear and unambiguous evidence to the contrary. Otherwise, voluminous and intimate data would be readily subject to indiscriminate police review. The consent exception, which was largely developed prior to the advent of phones that store enormous amounts of data, should not be used to expand access to digital data, which the U.S. Supreme Court has held should be subject to more, not less, Fourth Amendment protection. *Riley*, 573 U.S. at 393.

Courts evaluate consent for Fourth Amendment search purposes by asking whether the search was “voluntary,” which “is a question of fact to be determined from all the circumstances.” *Schneckloth v. Bustamonte*, 412 U.S. 218, 248–49 (1973). “No single criterion controls [the] decision.” *State v. Phillips*, 218 Wis. 2d 180, ¶ 26, 577 N.W.2d 794 (1998). “The State bears the burden of establishing, clearly and convincingly, that a warrantless search was reasonable and in compliance with the Fourth

Amendment.” *State v. Matejka*, 2001 WI 5, ¶ 18, 241 Wis. 2d 52, 621 N.W.2d 891.

With that in mind, common intuition about how cell phones work would limit consensual access to particular categories of data found on a device, rather than the entire corpus. When a person looks for information on their own cell phone, they commonly open a particular app, such as text messages or email. They then search that specific category of data, either by scrolling through messages or by typing a query term in the search bar and pressing “Enter.” The owner reasonably expects the same common-sense “search” when giving consent to police.

However, when police use a MDFT to search a phone, the individual “likely doesn’t even have a rough idea of what’s really about to happen to their phone.” Upturn Report at 60. The public generally does not know that MDFTs exist, how they work, or that police departments use them to conduct forensic searches of phones. Before Upturn’s report, there was essentially no public accounting of how often police use MDFTs, the broad range of investigations in which they do so, how much data they uncover, their analytic capabilities, and what happens with the data afterwards. If privacy experts are only beginning to pierce the veil of police MDFT use, ordinary citizens cannot be expected to understand and consent to extractive searches.

Under these circumstances, the layperson’s common-sense understanding that consent applies to particular categories of data on a device, and not to all information, should rule. *United States v. Morton* illustrates this point. 984 F.3d 421 (5th Cir. 2021). In *Morton*, given the nature of the crime, the court determined that probable cause was sufficient to support a warrant to search only certain aspects of a phone—but not others. *Id.* at 426. Noting that the Supreme Court’s decision in *Riley* rested in part on the observation that “a cell phone’s capacity allows even just one type of information to convey far more than previously possible,” the *Morton* court held that “*Riley* made clear that [ ] distinct types of information, often stored in different components of the phone, should be analyzed separately.” *Id.* Just as “[c]onsent to search a garage would not implicitly authorize a search of an adjoining house,” *Walter*, 447 U.S. at 656–57, consent

to search “information” on a phone is limited by the category of information made salient by the context of the consent.

This limitation on the categories of data that can be searched also applies to deleted information, information stored in the cloud, and data, such as incoming messages, that did not exist when law enforcement first received consent to search. Individuals generally do not give prospective consent to a search for information they did not know or expect to be on the phone. An ordinary person does not know that data they delete from their device is still “on” it and does not expect that anyone in possession of the phone can access deleted information. *See* Upturn Report at 21–22. Further, when a person deletes data from their phone, they clearly indicate that they do not want anyone, including law enforcement, to look at the data, thus excluding it from the scope of consent. Similarly, accessing data stored on the cloud and not actually resident on the device also dramatically expands the scope of a search. *Riley*, 573 U.S. at 397. As the *Riley* Court explained, “[t]reating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter. But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen.” *Id.* (citations omitted). Finally, information received while the phone is in law enforcement’s possession may change the individual’s decision to consent and thus cannot be considered within the scope of the original consent.

Here, the evidence shows that Burch gave consent only to a limited search of his text messages. In response to Detective Bourdelais’s inquiry about text messages that would corroborate his story that he was not in the neighborhood of the hit-and-run, Burch agreed that Detective Bourdelais could search those messages. *State v. Burch*, No. 2019AP1404-CR, at 3 (Wis. Ct. App. Oct. 20, 2020). Detective Bourdelais then inquired whether Burch would be willing to let the police download “the information” off the phone. *Id.* at 4. A reasonable person would have understood this to mean download “the information” they had previously discussed—the text messages.

**B. Consent searches are also limited in scope to the purposes for which a reasonable person would understand their data is being examined.**

When agreeing to a cell phone search, a reasonable person believes that they agree to a search for evidence of crimes related to the investigation at hand. Searches for evidence of unrelated crimes will generally be outside of the scope of consent and unconstitutional.

“The scope of a search is generally defined by its expressed object.” *Jimeno*, 500 U.S. at 251. In *Jimeno*, the officer told the defendant that he wanted to search his car for narcotics and the defendant consented. That consent necessarily included permission to search containers in the car that might hold drugs. *Id.* The consent does not include searches of areas of the car or packages which could not contain narcotics. Similarly, Burch’s consent to search his texts in connection with the hit-and-run does not cover different types of files, nor evidence of a different offense.

Inspections are “limited to the purposes contemplated by the [consenting] suspect.” *United States v. Blocker*, 104 F.3d 720, 728 (5th Cir. 1997) (quoting *United States v. Bosse*, 898 F.2d 113, 115 (9th Cir. 1990)). Police are not allowed to misrepresent the purpose for consent. If they do, the consent is invalid. “A ruse entry when the suspect is informed that the person seeking entry is a government agent but is misinformed as to the purpose for which the agent seeks entry cannot be justified by consent.” *Bosse*, 898 F.2d at 115. The searches here should have been limited to the purpose that Burch, or a reasonable person in his position, contemplated—evidence of the hit-and-run, and not some other crime.

**C. Limitations on consent are particularly important because consent searches of cell phones raise unique concerns about law enforcement coercion.**

People may feel coerced to offer consent when law enforcement seizes or threatens to search their cell phones. Scholars and practitioners have long criticized the consent exception to the Fourth Amendment’s warrant requirement on policy grounds, often referencing the inherently coercive nature of law enforcement “requests.” *See, e.g.,*

Marcy Strauss, *Reconstructing Consent*, 92 J. Crim. L. & Criminology 211, 236 (2002) (“most people would not feel free to deny a request by a police officer”); Janice Nadler, *No Need to Shout: Bus Sweeps and the Psych. of Coercion*, 2002 Sup. Ct. Rev. 153, 156 (2002) (“the fiction of consent in Fourth Amendment jurisprudence has led to suspicionless searches of many thousands of innocent citizens who ‘consent’ to searches under coercive circumstances”). Many have also observed that coercion is particularly present for people of color, and especially Black Americans, who may fear physical harm if they decline a request from a law enforcement officer. *See, e.g.*, Devon W. Carbado, *(E)Racing the Fourth Amend.*, 100 Mich. L. Rev. 946, 971, 972 & n.121, 973 (2002); *United States v. Washington*, 490 F.3d 765, 768–69 (9th Cir. 2007) (finding lack of consent after two incidents where white police officers shot African Americans during traffic stops).

In the cell phone context, people may feel additional coercion to consent to a search just to get their device back. Cell phones perform many essential functions, serving as prescription drug reminders,<sup>10</sup> and lifelines to app-based services such as Uber and Lyft. People who find themselves questioned by law enforcement may feel pressured to acquiesce to search requests to quickly regain access to the device, for example to call the babysitter and say that they’ve been delayed and will be home late.

**D. Consent forms deserve little weight because they often fail to provide people facing an investigation sufficient information about their rights or about what a search means.**

As the State concedes, “a general consent form can be overridden by more explicit statements.” State Br. at 17. In practice, consent forms should get little weight in determining the scope of consent in the mind of a reasonable person. Research shows both that consent forms fail to inform people of their rights and that most people do not read consent forms. Police often use generic consent forms to authorize broad forensic

---

<sup>10</sup> J.D. Biersdorfer, *Getting Alerts from a Digital Pillbox*, N.Y. Times (June 5, 2017), <https://perma.cc/M4DR-DABR>. (“The App Store stocks several dozen pharmaceutical apps designed to organize your pills, schedule doses and remind you to take your medicine.”).

phone searches. Most agencies' consent forms fail to specify how police search the phone, which tools they use, the scope of the search, how long they intend to retain the data, and the purposes to which that data may be put. Upturn Report at 60 & n.195. The form at issue in this case is a prime example. It purported to give "Officer Bourdelais or any assisting personnel permission to search my Samsung Cellphone." R. 234:12, App'x at 111; R. 78, App'x at 114. Consent forms that do not clearly describe the searches they supposedly authorize should not override evidence of a more limited scope of consent, such as the explicitly limited access to "text messages" that Burch gave in this case.

Further, a wide body of research shows that across different contexts, most people do not read consent forms. *See, e.g.,* Benjamin D. Douglas et al., *Some Rschs. Wear Yellow Pants, but Even Fewer Participants Read Consent Forms: Exploring and Improving Consent Form Reading in Human Subjects Rsch.*, 26 *Psych. Methods* 61 (2021) ("Participants do not thoroughly read, comprehend, or recall information in consent forms" in medical trials or procedures.). This is particularly true when the person is in police custody, under investigation, or otherwise confronted with the power of the state. "[A] consent form may do relatively little to improve a suspect's understanding of her rights, particularly when the suspect is poorly educated, frightened, or otherwise unable to understand the form." Nancy Leong & Kira Suyeishi, *Consent Forms and Consent Formalism*, 2013 *Wis. L. Rev.* 751, 753 (2013). Further, "once the suspect has been given the form, the inclination is merely to read it rather than to engage in a dialogue with the officer designed to clarify the meaning of the form." *Id.* at 789.

All of these factors mean written consent forms are not especially persuasive or binding evidence that a reasonable person consented to a particular search. Here, the existence of a signed consent form should not override Burch's limited verbal consent to search his text messages. The consent waiver Burch signed did not specify what areas of his phone would be searched, what tools would be used to conduct the search, or what would happen to his data following the search. *State v. Burch*, No. 2019AP1404-CR, at 4. Nor is there any indication in the record that Detective Bourdelais explained any of these things to Burch, which could have lent more weight to the form in a "totality of the

circumstances” analysis of the scope of consent. For these reasons, this Court should find that Burch’s consent to search his cell phone extended no further than his text messages.

### **III. THE RETENTION OF BURCH’S CELL PHONE DATA VIOLATED THE FOURTH AMENDMENT.**

The government’s ongoing retention of Burch’s cell phone data was unreasonable because it seized data outside of the scope of consent; it retained data that was non-responsive to the hit-and-run investigation;<sup>11</sup> and it retained the data after the State concluded that Burch was not a suspect in that investigation. At each of these points, the government had at most a limited interest in holding Burch’s data. Burch’s privacy interest in his own data dwarfed the State’s interest. Therefore, the seizure of Burch’s data was unreasonable and violated his Fourth Amendment rights.

#### **A. Copying Burch’s digital data constituted a seizure under the Fourth Amendment.**

By copying data on Burch’s phone, the Green Bay Police Department (“GBPD”) effected a seizure within the meaning of the Fourth Amendment. “A ‘seizure’ of property occurs when there is some meaningful interference with an individual’s possessory interests in that property.” *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). As Justice Stevens wrote in *United States v. Karo*, “[t]he owner of property, of course, has a right to exclude from it all the world, including the Government, and a concomitant right to use it exclusively for his own purposes.” 468 U.S. 705, 729 (1984) (Stevens, J., concurring in part and dissenting in part). Just as physical property may be “seized” within the meaning of the Fourth Amendment, so too may digital property. *See, e.g., United States v. Werdene*, 883 F.3d 204, 212 (3d Cir. 2018) (government software “seized” information from defendant’s computer); *United States v. Ganius*, 755 F.3d 199, 137 (2nd Cir. 2016) (en banc); *United States v. Comprehensive Drug Testing, Inc.*,

---

<sup>11</sup> “Responsive data” generally refers to information relevant to probable cause while “non-responsive data” means irrelevant information police were nevertheless permitted to overseize as a matter of administrative convenience. Here, we use “non-responsive data” to include information other than the text message data as well as any data on the phone that did not relate to the initial hit-and-run investigation.

621 F.3d 1162 (9th Cir. 2010) [hereinafter *CDT*] (en banc) (per curiam) (referring to the copying of electronic data as a seizure throughout the opinion).

When the GBPD copied the contents of Burch's phone, they deprived him of core possessory interests: the rights to exclude others from using his data and to dispose of his data as he saw fit. The Brown County Sheriff's Office ("BCSO") repeated these deprivations when it obtained another copy of the data from the GBPD. These acts of copying constituted two separate seizures under the Fourth Amendment.

**B. It was unreasonable for the State to retain everything on Burch's phone.**

The Supreme Court has made clear that "a seizure lawful at its inception can nevertheless violate the Fourth Amendment because its manner of execution unreasonably infringes possessory interests protected by the Fourth Amendment[]." *Jacobsen*, 466 U.S. at 124. To determine whether a given seizure is reasonable under the Fourth Amendment, the Court looks to whether it "was reasonably related in scope to the circumstances which justified the interference in the first place." *Terry v. Ohio*, 392 U.S. 1, 20 (1968). Thus, in *United States v. Place*, for example, the Court held that although an initial seizure of luggage for the purpose of subjecting it to a "dog sniff" test was reasonable, prolonging that detention by ninety minutes was "sufficient to render the seizure unreasonable." 462 U.S. 696, 710 (1983); *see also Jacobsen*, 466 U.S. at 124 n.25 ("The seizure became unreasonable because its length unduly intruded upon constitutionally protected interests.").

The recognition that an initially justified seizure may become unreasonable solely due to ongoing detention is particularly important in cases involving the search of electronic devices. Because evidence on these devices may be intermingled with a large amount of irrelevant data, courts frequently permit the government to initially seize data beyond the scope of its authorization to facilitate later targeted searches. *See, e.g., CDT*, 621 F.3d at 1177 (recognizing the "reality that over-seizing is an inherent part of the electronic search process"). But the government does not have an independent right to hold the data it gains through overseizure; that data is instead obtained through "a

courtesy that was developed for law enforcement.” *People v. Thompson*, 28 N.Y.S.3d 237, 259 (N.Y. Sup. Ct. 2016); see *United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982) (“[T]he wholesale *seizure* for later detailed examination of records not described in a warrant is significantly more intrusive, and has been characterized as ‘the kind of investigatory dragnet that the [F]ourth [A]mendment was designed to prevent.’” (citation omitted)).

Thus, the Fourth Amendment does not allow the government to profit from its overseizure of digital data. See *CDT*, 621 F.3d at 1177 (declaring in context of search authorized by warrant “[t]he process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect.”). When the government overseizes data as part of a device search, “[t]he potential for privacy violations occasioned by an [additional] unbridled, exploratory search . . . is enormous,” *United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013). As a result, the Fourth Amendment particularity requirement “assumes even greater importance” where digital evidence is concerned than it does in the physical evidence context. *Id.* at 446.

The U.S. Supreme Court has articulated a balancing test to determine when a seizure becomes unreasonable. Courts “must balance the nature and quality of the intrusion on the individual’s Fourth Amendment interests against the importance of the governmental interests alleged to justify the intrusion.” *Jacobsen*, 466 U.S. at 125 (citation omitted). The same balancing test can be used to determine the reasonableness of the government’s seizure and continued retention of individuals’ digital data.

Because a person’s privacy and possessory interests in the whole of the electronic data on a device are of the highest significance—these devices “hold for many Americans the ‘privacies of life,’” *Riley*, 573 U.S. at 403 (citation omitted)—courts must apply intense scrutiny to the government’s asserted interests and ensure the government intrusion is properly cabined. The government may have an interest in initially oversteering data so that, for example, it can later use the proper search tools and does not have to effectuate a targeted search on site. Here, the forensic investigator created a

report containing all communications back and forth after June 7. *See* State Br. at 11. Even if the GBPD were justified in initially overseizing Burch’s data—for example, if this Court were to find that Burch’s consent extended beyond his text messages—after the police generated the report, the agency’s legitimate interests in retaining the rest of Burch’s data were minimal. *See United States v. Metter*, 860 F. Supp. 2d 205, 212 (E.D.N.Y. 2012) (government’s fifteen-month delay in reviewing seized electronic evidence and segregating non-responsive data was unreasonable).

The GBPD’s interests in retaining Burch’s data were diminished even further when he was no longer a suspect.<sup>12</sup> The State has offered no good reason for keeping the data contained in the hit-and-run report, never mind the entirety of the data. Because Burch was no longer a suspect and the data on his phone was irrelevant to the investigation of any other suspect, the State’s argument that it needed to retain all of Burch’s data to properly authenticate the download, State Br. at 22–24, fails. At that point, Burch’s privacy and possessory interests in his data outweighed the government’s interests, and any retention of data outside the scope of the first investigation—at least any data not included in the report—was unreasonable.

### **C. The Fourth Amendment requires that law enforcement purge or return unreasonably seized digital data.**

To effectuate the Fourth Amendment’s guarantee against unreasonable seizures, this Court should require that law enforcement purge unreasonably seized data. The rule is a straightforward application of the Supreme Court’s decision in *Andresen v. Maryland*, 427 U.S. 463 (1976).<sup>13</sup> There, the Supreme Court affirmed that with respect to

---

<sup>12</sup> The State argues that the record does not clearly demonstrate whether or not the hit-and-run investigation was over. Even if true, the burden of justifying a warrantless search or seizure falls on the government, not on the defendant. *Kentucky v. King*, 563 U.S. 452, 474 (2011).

<sup>13</sup> This approach is also consistent with common understanding at the time of the Framers. A recent scholarly article establishes that the Framers understood that seized evidence had to be brought before a magistrate who then had the authority to return evidence seized outside of the scope of a warrant to the property owner. *See* Laurent Sacharoff, *The Fourth Amend. Inventory as a Check on Digit. Searches*, 105 Iowa L. Rev. 1643, 1687 (2020) (“[T]he original practice provides a surprisingly unambiguous picture of the central role the return played in England and the colonies, both as ordinary practice and as important rhetoric leading to the Fourth Amendment.”).

papers that exceeded the scope authorized by the government’s search warrant, “the State was correct in returning them voluntarily,” *Id.* at 482 n.11. The same rule that covers paper records that the government has no right to hold—that they must be returned to the full control of their owner—applies also to digital data. Even the U.S. Department of Justice has recognized that the government has a duty to purge non-responsive files. *See Ganius*, 824 F.3d at 238 (Chin, J., dissenting) (government agent acknowledged he should have returned or destroyed non-responsive items after a “reasonable period” of off-site review). Lastly, several federal courts have drawn a purge requirement from the Fourth Amendment as they have denied warrant applications on the grounds that the government did not adequately establish a procedure to purge data beyond the scope of the authorization. *See In re Search of Black iPhone 4*, 27 F. Supp. 3d 74, 80 (D.D.C. 2014); *In re Search of Info. Associated with the Facebook Acct. Identified by the Username Aaron.Alexis That Is Stored at Premises Controlled by Facebook, Inc.*, 21 F. Supp. 3d 1, 10 (D.D.C. 2013); *In the Matter of the Search of Premises Known as a Nextel Cellular Tel.*, No. 14-MJ-8005-DJW, 2014 WL 2898262, at \*10 (D. Kan. June 26, 2014); *Matter of the Search of Apple iPhone, IMEI 013888003738427*, 31 F. Supp. 3d 159, 166 (D.D.C. 2014); *Matter of Search of ODYS LOOX Plus Tablet Serial No. 4707213703415 in Custody of United States Postal Inspection Serv., 1400 New York Ave NW, Washington, DC*, 28 F. Supp. 3d 40, 45 (D.D.C. 2014).<sup>14</sup>

In the alternative, this Court should follow the Oregon Supreme Court in imposing a restriction on law enforcement’s ability to use any evidence that exceeds its authorization to search. *State v. Mansor*, 421 P.3d 323, 342–43 (Or. 2018). A use restriction would limit the government, except in exigent circumstances and other narrow exceptions, to using only data that is actually responsive to—that is, described by—the

---

<sup>14</sup> The Fourth Amendment does not require Burch to make a formal request for the return of his data because the government has no legal basis to retain information it has no authorization to hold. *See Ganius*, 824 F.3d at 236 (Chin, J., dissenting) (noting that government, not defendant, bears burden of proving reasonableness under Fourth Amendment). The availability of statutory procedures that provide for the return of property has no bearing on the constitutional requirements.

warrant (or within the scope of consent in this case). As one influential commentator has explained, “[t]his approach best reconciles the government’s compelling need to obtain the evidence sought in the warrant with the Fourth Amendment’s prohibition on general warrants.” Orin S. Kerr, *Executing Warrants for Digit. Evid.: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex. Tech. L. Rev. 1, 10 (2015). While a purge rule is more privacy protective and protects against the problem of “parallel construction” whereby the government builds an independent evidentiary basis to conceal the original source of unlawfully obtained evidence, under either approach, the Court must ensure that “future searches of electronic records” do not turn “all warrants for digital data into general warrants.” *CDT*, 621 F.3d at 1178 (Kozinski, J., concurring); *see also United States v. Sedaghaty*, 728 F.3d 885, 914 (9th Cir. 2013) (invalidating computer search where agents sought to retain and use “information beyond the scope of the warrant” and insisting that agents “should have sought a further warrant”).

#### **IV. THE BROWN COUNTY SHERIFF OFFICE’S SUBSEQUENT SEARCH OF BURCH’S DATA VIOLATED THE FOURTH AMENDMENT.**

Because the retention of Burch’s phone was unlawful, this Court need not reach the issue of the Brown County Sherriff’s Office (BCSO) subsequent search of the cell phone data. Nonetheless, the BCSO’s search of Burch’s data pursuant to its investigation of a wholly unrelated crime constituted an independent violation of the Fourth Amendment. Not only was this search executed on data the government no longer had authority to retain, it was conducted without a warrant. *See, e.g., Ganius*, 824 F.3d at 199 (finding good faith reliance on second search warrant immunized government’s retention and search of defendant’s data in later, unrelated investigation); *see also United States v. Wey*, 256 F. Supp. 3d 355, 407 (S.D.N.Y. 2017) (Fourth Amendment violated when law enforcement mined overseized information for evidence of new crimes); *United States v. Hulscher*, No. 4:16-CR-40070-01-KES, 2017 WL 657436, at \*3 (D.S.D. Feb. 17, 2017) (finding second search warrant necessary to investigate wholly separate set of crimes and noting that to find otherwise “would allow for mass retention of unresponsive cell phone data [and] is simply inconsistent with the protections of the Fourth Amendment”).

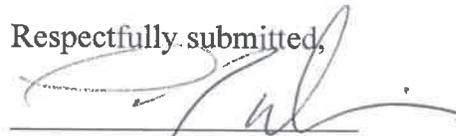
As even the State acknowledges, the police's authority to "subsequently examine an item lawfully in their possession" extends only "to the same extent they could originally search the item." State Br. at 26. That is also consistent with the lead opinion in *Randall*, 2019 WI 80, ¶ 35 (consent to search lawfully obtained blood sample for alcohol content does not provide authorization to search for "genetic information"). Because searching for evidence of an unrelated crime far exceeds the scope of Burch's authorization, even if GBPD lawfully could have retained a copy of Burch's data, the BCSO was obligated to obtain a second warrant to search it.

### CONCLUSION

This Court should reverse the decision below and remand for a new trial.

Dated this 4th of March, 2021.

Respectfully submitted,



Laurence J. Dupuis (WBN 1029261)  
Legal Director  
American Civil Liberties Union of  
Wisconsin Foundation  
207 E. Buffalo Street, Suite 325  
Milwaukee, WI 53202  
Telephone: (414) 272-4032, ext. 212  
Email: ldupuis@aclu-wi.org

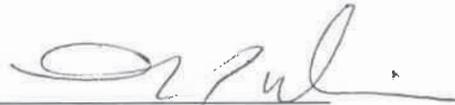
Jennifer Granick, admitted *pro hac vice*  
American Civil Liberties  
Union Foundation  
39 Drumm Street  
San Francisco, CA 94111  
Telephone: (415) 343-0758  
Email: jgranick@aclu.org

Jennifer Lynch, admitted *pro hac vice*  
Electronic Frontier Foundation  
815 Eddy Street  
San Francisco, CA 94109  
Telephone: (415) 436-9333  
Email: jlynch@eff.org

**CERTIFICATION AS TO FORM AND LENGTH**

I hereby certify that this brief conforms to the rules contained in Wis. Stat. § 809.19(8)(b) and (c) for a brief produced with a proportional serif font. The length of this brief is 7,500 words, permitted per order of this Court issued on February 18, 2021.

Dated this 4th of March, 2021



Laurence J. Dupuis (WBN 1029261)  
Legal Director  
American Civil Liberties Union of  
Wisconsin Foundation  
207 E. Buffalo Street, Suite 325  
Milwaukee, WI 53202  
Telephone: (414) 272-4032, ext. 212  
Email: ldupuis@aclu-wi.org

**CERTIFICATE OF COMPLIANCE WITH WIS. STAT. § 809.19(12)**

I hereby certify that:

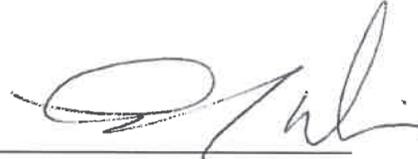
I have submitted an electronic copy of this brief, excluding the appendix, if any, which complies with the requirements of Wis. Stat. § 809.19(12).

I further certify that:

This electronic brief is identical in content and format to the printed form of the brief filed as of this date.

A copy of this certificate has been served with the paper copies of this brief filed with the Court and served on all parties.

Dated this 4th of March, 2021



Laurence J. Dupuis (WBN 1029261)  
Legal Director  
American Civil Liberties Union of  
Wisconsin Foundation  
207 E. Buffalo Street, Suite 325  
Milwaukee, WI 53202  
Telephone: (414) 272-4032, ext. 212  
Email: ldupuis@aclu-wi.org

# SUPREME COURT OF WISCONSIN

CASE No.: 2019AP1404-CR

COMPLETE TITLE: State of Wisconsin,  
 Plaintiff-Respondent,  
 v.  
 George Steven Burch,  
 Defendant-Appellant.

ON CERTIFICATION FROM THE COURT OF APPEALS

OPINION FILED: June 29, 2021  
 SUBMITTED ON BRIEFS:  
 ORAL ARGUMENT: April 12, 2021

SOURCE OF APPEAL:  
 COURT: Circuit  
 COUNTY: Brown  
 JUDGE: John Zakowski

JUSTICES:

HAGEDORN, J., delivered the majority opinion of the Court, in which ZIEGLER, C.J, ROGGENSACK, and REBECCA GRASSL BRADLEY, JJ., joined, and in which DALLET and KAROFISKY, JJ., joined with respect to Parts I. and II.B. REBECCA GRASSL BRADLEY, J., filed a concurring opinion. DALLET, J., filed an opinion concurring in part and dissenting in part, in which KAROFISKY, J., joined and in which ANN WALSH BRADLEY, J., joined except for footnote 1. ANN WALSH BRADLEY, J., filed a dissenting opinion.

NOT PARTICIPATING:

ATTORNEYS:

For the defendant-appellant, there were briefs filed by *Ana L. Babcock* and *Babcock Law, LLC*. There was an oral argument by *Ana L. Babcock*.

For the plaintiff-respondent, there was a brief filed by *Aaron R. O'Neil*, assistant attorney general; with whom on the brief was *Joshua L. Kaul*, attorney general. There was an oral argument by *Aaron R. O'Neil*.

An amicus curiae brief was filed on behalf of *Legal Action of Wisconsin, Inc.* by *Rebecca M. Donaldson*, Milwaukee.

An amicus curiae brief was filed on behalf of *American Civil Liberties Union Foundation*, *American Civil Liberties Union of Wisconsin Foundation*, *Electronic Frontier Foundation*, and *Electronic Privacy Information Center* by *Laurence J. Dupuis* and *American Civil Liberties Union of Wisconsin Foundation*, Milwaukee; with whom on the brief was *Jennifer Granick* and *American Civil Liberties Union Foundation*, San Francisco, California; with whom on the brief was *Jennifer Lynch* and *Electronic Frontier Foundation*, San Francisco, California.

2021 WI 68

NOTICE

This opinion is subject to further editing and modification. The final version will appear in the bound volume of the official reports.

No. 2019AP1404-CR  
(L.C. No. 2016CF1309)

STATE OF WISCONSIN

:

IN SUPREME COURT

---

**State of Wisconsin,**

**Plaintiff-Respondent,**

**v.**

**George Steven Burch,**

**Defendant-Appellant.**

**FILED**

**JUN 29, 2021**

Sheila T. Reiff  
Clerk of Supreme Court

---

HAGEDORN, J., delivered the majority opinion of the Court, in which ZIEGLER, C.J, ROGGENSACK, and REBECCA GRASSL BRADLEY, JJ., joined, and in which DALLET and KAROFKY, JJ., joined with respect to Parts I. and II.B. REBECCA GRASSL BRADLEY, J., filed a concurring opinion. DALLET, J., filed an opinion concurring in part and dissenting in part, in which KAROFKY, J., joined and in which ANN WALSH BRADLEY, J., joined except for footnote 1. ANN WALSH BRADLEY, J., filed a dissenting opinion.

---

APPEAL from a judgment of the Circuit Court for Brown County. *Affirmed.*

¶1 BRIAN HAGEDORN, J. George Steven Burch appeals a judgment of conviction for first-degree intentional homicide on the grounds that two pre-trial evidentiary motions were incorrectly denied.

**APPENDIX 201**

¶2 First, relying on the Fourth Amendment, Burch moved to suppress the admission of incriminating cell phone data. This data was obtained via an unrelated criminal investigation and kept in a police database. A different law enforcement agency investigating the homicide came upon this data and used it to connect Burch to the homicide. Burch argues that the initial download of the data exceeded the scope of his consent, the data was unlawfully retained, and the subsequent accessing of the data violated his reasonable expectation of privacy. We conclude that even if some constitutional defect attended either the initial download or subsequent accessing of the cell phone data, there was no law enforcement misconduct that would warrant exclusion of that data. Therefore, we conclude the circuit court correctly denied Burch's motion to suppress that data.

¶3 Regarding the second pre-trial evidentiary motion, Burch asks us to reverse the circuit court's discretionary decision to admit evidence from a Fitbit device allegedly worn by the victim's boyfriend at the time of the homicide. This evidence, Burch maintains, should have been accompanied by expert testimony and was insufficiently authenticated. We agree with the State that the circuit court's decision to admit this evidence was not an erroneous exercise of discretion. Burch's judgment of conviction is affirmed.

#### I. BACKGROUND

¶4 On May 20, 2016, Nicole VanderHeyden went to a bar with her boyfriend, Douglass Detrie. The two became separated

and, in the course of a subsequent phone call and text messages, got into an argument. Detrie returned alone to their shared home. The next day, VanderHeyden's body was discovered next to a nearby field. Her blood-stained clothing was later found discarded alongside a freeway on-ramp, and some of her blood and hair were identified outside the house of VanderHeyden's neighbor. The Brown County Sheriff's Office (the "Sheriff's Office") opened a homicide investigation that spanned the next several months. Detrie was initially a suspect, but the focus of the investigation shifted away from Detrie in part because his Fitbit device logged only 12 steps during the hours of VanderHeyden's death.<sup>1</sup>

¶5 While the Sheriff's Office investigated VanderHeyden's homicide, the Green Bay Police Department (the "Police Department") undertook an unrelated investigation into three incidents involving the same vehicle—a stolen vehicle report, a vehicle fire, and a hit-and-run. George Burch was a suspect in this investigation, and Police Department Officer Robert Bourdelais interviewed him on June 8, 2016. Burch denied involvement and offered the alibi that he was at a bar that night and texting a woman who lived nearby. As Officer Bourdelais testified, "I asked [Burch] if I could see the text messages between him and [the woman], if my lieutenant and I could take a look at his text messages." Burch agreed. Officer

---

<sup>1</sup> Detrie wore a Fitbit Flex, a wrist-worn device that continuously tracks the wearer's steps and interfaces with the wearer's phone or computer.

Bourdelaais then explained that he preferred to download information off the phone because "it's a lot easier to do that than try to take a bunch of pictures and then have to scan those in." "So I asked him if he would be willing to let me take his phone to this detective, download the information off the phone and then I'd bring the phone right back to him . . . and he said that would be fine."

¶6 Before Officer Bourdelaais took the phone to be downloaded, Burch signed a consent form. The form read: "I George Stephen Burch . . . voluntarily give Det. Danielski, Officer Bourdelaais or any assisting personnel permission to search my . . . Samsung cellphone." Officer Bourdelaais took the phone and the signed consent form to the certified forensic computer examiner for the Police Department. The forensic expert performed a "physical extraction" of all the data on Burch's phone, brought the data into a readable format, and saved the extraction to the Police Department's long-term storage. At a motion hearing, the forensic expert testified that this was consistent with the Police Department's standard practice.

¶7 Two months later, two Sheriff's Office detectives continuing the investigation of VanderHeyden's homicide matched a DNA sample from VanderHeyden's sock to Burch. The detectives then searched their own department's records and the records of other local departments for prior police contacts with Burch. There they discovered the Police Department's file related to the three vehicle-related incidents. The file included Burch's

signed consent form and a copy of the data the Police Department extracted from Burch's phone during the search. It also contained a narrative written by Officer Bourdelais which indicated Burch said Officer Bourdelais "could take his phone to the department to have the information on it downloaded." Nothing in the consent form, the narrative, or anything else in the file, indicated that Burch limited the scope of the data he consented to have downloaded from his phone.

¶8 The Sheriff's Office detectives reviewed the data downloaded from Burch's phone. They noted that Burch's internet history included 64 viewings of news stories about VanderHeyden's death. And they also discovered Burch had an email address associated with a Google account. In light of this discovery, the Sheriff's Office detectives procured a search warrant to obtain the "Google Dashboard" information from Google corresponding to Burch's email address. The data Google provided contained location information that placed Burch's phone at a bar VanderHeyden visited the night of her death, a location near VanderHeyden's residence, the place where VanderHeyden's body was found, and the on-ramp where VanderHeyden's discarded clothing was discovered.

¶9 Burch was arrested and charged with VanderHeyden's death. He filed two pre-trial evidentiary motions relevant to this appeal.

¶10 In one motion, Burch sought to suppress the data obtained from his cell phone for two reasons: (1) the Police Department's extraction of the data exceeded the scope of

Burch's consent by obtaining all the phone's data, rather than just the text messages; and (2) the Sheriff's Office unlawfully accessed the data in August 2016. The circuit court<sup>2</sup> denied Burch's motion. It concluded that the conversation between Burch and Officer Bourdelais did not limit the scope of Burch's consent, and that "the sharing of such information, without first obtaining a warrant, is a common and long-understood practice between related departments."

¶11 Burch also moved to exclude evidence related to Detrie's Fitbit device. He argued the State must produce an expert to establish the reliability of the science underlying the Fitbit device's technology and that the State failed to sufficiently authenticate the records. The circuit court disagreed and refused to exclude the Fitbit evidence related to step-counting.<sup>3</sup>

¶12 Burch testified in his own defense at trial. He denied killing VanderHeyden, but acknowledged he was with her the night she died. According to Burch, he met VanderHeyden at a bar, and the two left together. After parking near VanderHeyden's house, they became intimate. That, Burch said, was the last thing he remembered before waking up on the ground with Detrie there, and VanderHeyden dead. Burch told the jury that Detrie held him at gunpoint and instructed him to move

---

<sup>2</sup> The Honorable John P. Zakowski of the Brown County Circuit Court presided.

<sup>3</sup> The circuit court granted Burch's motion in part, agreeing to exclude Fitbit evidence related to sleep-monitoring.

VanderHeyden's body into his vehicle, drive to a field, and carry VanderHeyden's body into the ditch. Only then did Burch escape by pushing Detrie, running back to his vehicle, and driving away. Burch added that on his way home he noticed that articles of VanderHeyden's clothing were still in his vehicle and threw them out the window in a panic. In the months that followed, Burch told no one this version of events, even as authorities sought the public's help in solving VanderHeyden's homicide.

¶13 The jury found Burch guilty of first-degree intentional homicide, and the circuit court sentenced him to life in prison. Burch appealed, challenging the circuit court's denial of his motion to suppress the cell phone data and his motion to exclude the Fitbit evidence. The court of appeals certified the case to us, and we accepted the certification.

## II. DISCUSSION

### A. Cell Phone Data

¶14 Burch asks us to reverse the circuit court's denial of his motion to suppress the cell phone data as contrary to the Fourth Amendment. The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. On review of a circuit court's denial of a suppression motion, we uphold the circuit court's findings of historical fact unless they are clearly erroneous, and independently apply constitutional principles to those facts.

State v. Robinson, 2010 WI 80, ¶22, 327 Wis. 2d 302, 786 N.W.2d 463.

¶15 Before us, Burch argues the cell phone data was obtained in violation of the Fourth Amendment for three reasons: (1) the Police Department obtained the data without his consent; (2) the Police Department unlawfully retained the data after its investigation into the vehicle-related incidents had ended; and (3) the Sheriff's Office unlawfully accessed the data in the Police Department's records without a warrant.<sup>4</sup> However, for the reasons that follow, regardless of whether the data was unlawfully obtained or accessed, we conclude suppression of the data is not warranted under the exclusionary rule. See Herring v. United States, 555 U.S. 135, 139 (2009) (accepting the "assumption that there was a Fourth Amendment violation" and analyzing whether the exclusionary rule applied); see also State v. Kerr, 2018 WI 87, ¶¶20-24, 383 Wis. 2d 306, 913 N.W.2d 787.

#### 1. The Exclusionary Rule

¶16 "When there has been an unlawful search, a common judicial remedy for the constitutional error is exclusion." State v. Dearborn, 2010 WI 84, ¶15, 327 Wis. 2d 252, 786

---

<sup>4</sup> Burch forfeited his argument related to the Police Department's retention of the cell phone data by not raising that argument before the circuit court. See State v. Huebner, 2000 WI 59, ¶10, 235 Wis. 2d 486, 611 N.W. 2d 727. His arguments regarding the initial download of the data and the subsequent accessing of the data are, however, properly before us.

N.W.2d 97. The exclusionary rule is a judicially-created, prudential doctrine designed to compel respect for the Fourth Amendment's constitutional guaranty. Davis v. United States, 564 U.S. 229, 236 (2011). In recent years, the United States Supreme Court has significantly clarified the purpose and proper application of the exclusionary rule. See id.; Herring, 555 U.S. 135. In Davis, the Supreme Court explained that prior cases suggested that the exclusionary rule "was a self-executing mandate implicit in the Fourth Amendment itself." 564 U.S. at 237. However, more recent cases have acknowledged that the exclusionary rule is not one of "reflexive" application, but is to be applied only after a "rigorous weighing of its costs and deterrence benefits." Id. at 238. Thus, in both Herring and Davis, the Court explained that to "trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." Herring, 555 U.S. at 144; see also Davis, 564 U.S. at 240.

¶17 The "sole purpose" of the exclusionary rule "is to deter future Fourth Amendment violations." Davis, 564 U.S. at 236-37. Therefore, exclusion is warranted only where there is some present police misconduct, and where suppression will appreciably deter that type of misconduct in the future. Id. at 237. The exclusionary rule applies only to police misconduct that can be "most efficaciously" deterred by exclusion. Id. (quoting United States v. Calandra, 414 U.S. 338, 348 (1974)).

Specifically, "the exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence." Herring, 555 U.S. at 144. "But when the police act with an objectively reasonable good-faith belief that their conduct is lawful, or when their conduct involves only simple, isolated negligence, the deterrence rationale loses much of its force, and exclusion cannot pay its way." Davis, 564 U.S. at 238 (cleaned up).

¶18 "Real deterrent value is a 'necessary condition for exclusion,' but it is not 'a sufficient' one." Id. at 237 (quoting Hudson v. Michigan, 547 U.S. 586, 596 (2006)). In Davis, the Court explained that the "analysis must also account for the 'substantial social costs' generated by the rule." Id. (quoting United States v. Leon, 468 U.S. 897, 907 (1984)). It elaborated:

Exclusion exacts a heavy toll on both the judicial system and society at large. It almost always requires courts to ignore reliable, trustworthy evidence bearing on guilt or innocence. And its bottom-line effect, in many cases, is to suppress the truth and set the criminal loose in the community without punishment. Our cases hold that society must swallow this bitter pill when necessary, but only as a "last resort." For exclusion to be appropriate, the deterrence benefits of suppression must outweigh its heavy costs.

Id. (citations omitted).

¶19 Applying this rationale, the Supreme Court in Herring held that a county's failure to update a computer database to reflect the recall of an arrest warrant was only negligent, and therefore was "not enough by itself to require 'the extreme

sanction of exclusion.'" 555 U.S. at 140 (quoting Leon, 468 U.S. at 916). Similarly, in Davis, the Supreme Court refused to exclude evidence that was obtained via a search conducted in compliance with binding, but subsequently overruled, precedent. 564 U.S. at 232. Exclusion, it explained, was inappropriate because it "would do nothing to deter police misconduct." Id.

¶20 We have followed suit as well. In Kerr, we explained that no police misconduct occurred when an officer conducted an arrest relying on dispatch's confirmation that the defendant had a warrant out for his arrest. 383 Wis. 2d 306, ¶22. Exclusion was improper because "the officers' conduct [was] at most negligent, and isolated negligence is not 'misconduct' for purposes of the exclusionary rule." Id. (citing Herring, 555 U.S. at 146-47).

¶21 Many more examples could be provided,<sup>5</sup> but the principle is clear: unless evidence was obtained by sufficiently deliberate and sufficiently culpable police misconduct, "[r]esort to the massive remedy of suppressing

---

<sup>5</sup> See, e.g., United States v. Leon, 468 U.S. 897, 916 (1984) (reasonable reliance on a warrant later held invalid); Illinois v. Krull, 480 U.S. 340, 342 (1987) (reasonable reliance on subsequently invalidated statutes); Arizona v. Evans, 514 U.S. 1, 15-16 (1995) (reasonable reliance on arrest warrant information in a database maintained by judicial employees); State v. Ward, 2000 WI 3, ¶63, 231 Wis. 2d 723, 604 N.W.2d 517 (reasonable reliance on settled law subsequently overruled); State v. Dearborn, 2010 WI 84, ¶44, 327 Wis. 2d 252, 786 N.W.2d 97 (refusing to exclude evidence where doing so "would have absolutely no deterrent effect on officer misconduct").

evidence of guilt is unjustified."<sup>6</sup> Hudson, 547 U.S. at 599. With these principles in mind, we turn to the facts at hand.

## 2. Application

¶22 In this case, the Sheriff's Office detectives acted by the book. After a DNA sample from VanderHeyden's sock matched Burch, officers checked the interdepartmental records already on file with the police.<sup>7</sup> They discovered the two-month-old Police Department file documenting the investigation for the vehicle-related incidents. In it, they found and reviewed Burch's signed consent form and Officer Bourdelais' narrative further documenting Burch's consent. The Sheriff's Office detectives observed that neither the consent form nor the narrative listed any limitations to the scope of consent. And the officers reviewed the downloaded data, having every reason to think it was lawfully obtained with Burch's unqualified consent.

¶23 Burch argues that the Sheriff's Office should have obtained a warrant before accessing the Police Department's

---

<sup>6</sup> Failure to apply exclusion is usually described in our cases as the "good faith" exception to the exclusionary rule. See, e.g., Dearborn, 327 Wis. 2d 252, ¶4. However, the United States Supreme Court has called the "good faith" label confusing. Herring v. United States, 555 U.S. 135, 142 (2009). The Supreme Court's most recent cases do not use that phrase as a catchall for cases where exclusion is improper, and do not describe their conclusion that exclusion was inappropriate as applying a "good faith" exception. See id. at 147-48; Davis v. United States, 564 U.S. 229, 249-50 (2011).

<sup>7</sup> Officers from both the Police Department and the Sheriff's Office testified that it is common police practice for agencies to share records with other agencies.

data. But no case from this court or the federal courts has suggested that accessing evidence previously obtained by a sister law enforcement agency is a new search triggering a renewed warrant requirement.<sup>8</sup> Rather, the Sheriff's Office detectives reasonably relied on Burch's signed consent form and Officer Bourdelais' narrative to conclude that Burch consented to the download of the data. They had no reason to think they were engaging in illegal activity by reviewing interdepartmental files and evidence. Far from it. Reliance on well-documented computer records, like the detectives did here, is something the Supreme Court has characterized as objectively reasonable police conduct. Arizona v. Evans, 514 U.S. 1, 15-16 (1995). Thus, there was no misconduct that would "render[] the evidence suppressible under the exclusionary rule." Kerr, 383 Wis. 2d 306, ¶22.

¶24 Moreover, even if the Sheriff's Office's actions could be labeled as some kind of misconduct, nothing they did would rise beyond mere negligence. See id., ¶22 (concluding that "to the extent that looking at a warrant before executing it may be

---

<sup>8</sup> Justice Dallet's concurrence/dissent argues that courts should treat cell phone data collected by law enforcement differently than other types of evidence. It acknowledges that the sharing of already-collected evidence without a warrant by sister law enforcement agencies is routine and unproblematic, but maintains a different kind of analysis should attend cell phone evidence. We need not decide this question to conclude exclusion is not warranted in this case. Justice Dallet's approach would break new ground in Fourth Amendment jurisprudence, and as such, the violation of her new proposed rule does not implicate the kind of gross or systemic law enforcement misconduct the exclusionary rule is meant to deter.

best practice," failing to do so was "at most negligent"); Herring, 555 U.S. at 140 (holding that a county's failure to update a computer database was negligent and therefore "not enough by itself to require" exclusion). And mere negligence does not warrant suppression. Id. at 144-45.

¶25 In addition, the societal cost of excluding the cell phone data would far outweigh any deterrence benefit that exclusion might provide. See Dearborn, 327 Wis. 2d 252, ¶35. This is in part because there is nothing concerning under current Fourth Amendment doctrine with how the Sheriff's Office detectives conducted themselves. Even if the Police Department's initial download or retention gave cause for concern, it's not clear what behavior by the Sheriff's Office Burch would have this court seek to deter.<sup>9</sup> Based on the arguments presented, Burch has given us no reason to deter law enforcement reliance on the computer records of other law enforcement agencies. In this case, the societal cost of

---

<sup>9</sup> Many of Burch's arguments focus on the conduct of the Police Department and the initial download of his cell phone data. He argues that because the Police Department unlawfully obtained the data, any subsequent accessing of the data violated the Fourth Amendment because he retained a reasonable expectation of privacy in it. But the conduct of the Police Department has little bearing on whether we should apply the exclusionary rule against the Sheriff's Office in this case. The Police Department's involvement in this case was limited to an investigation of unrelated crimes and was only fortuitously useful to the Sheriff's Office's investigation of VanderHeyden's homicide months later. Exclusion therefore would not serve as a meaningful deterrent for the Police Department and is not warranted on that basis.

exclusion would far outweigh the limited benefit—if any—its application could achieve.

¶26 We conclude that suppression of Burch's cell phone data is not warranted under the exclusionary rule. Regardless of whether a constitutional violation occurred, there was no police misconduct to trigger application of the exclusionary rule.

#### B. Fitbit Evidence

¶27 Burch also appeals the circuit court's denial of his motion to exclude evidence associated with Detrie's Fitbit device. Burch offers two arguments. First, he argues the Fitbit evidence must be excluded because the State did not produce expert testimony to establish its reliability. Second, he maintains the Fitbit evidence was insufficiently authenticated.<sup>10</sup> We review these evidentiary rulings for an erroneous exercise of discretion. State v. Nelis, 2007 WI 58, ¶26, 300 Wis. 2d 415, 733 N.W.2d 619.

---

<sup>10</sup> Burch also argues that admission of the Fitbit evidence violates the Confrontation Clause of the Sixth Amendment to the United States Constitution. Burch concedes, however, that his novel argument "does not neatly fit within the test set forth in Crawford v. Washington, 541 U.S. 36 (2004)," and that he raised the issue solely "to preserve for review before higher courts." Accordingly, we reject Burch's Confrontation Clause claim and do not address it further.

## 1. Expert Testimony

¶28 We have held that that "the requirement of expert testimony is an extraordinary one" and should apply only "when the issues before the jury are 'unusually complex or esoteric.'" State v. Kandutsch, 2011 WI 78, ¶28, 336 Wis. 2d 478, 799 N.W.2d 865 (quoting another source). Before compelling expert testimony, "the circuit court must first find that the underlying issue is 'not within the realm of the ordinary experience of mankind.'" Id. (quoting Cramer v. Theda Clark Mem'l Hosp., 45 Wis. 2d 147, 150, 172 N.W.2d 427 (1969)). What falls within the "ordinary experience of mankind," meanwhile, turns on the circuit court's exercise of its discretion "on a case-by-case basis" to decide whether "the issue is outside the realm of lay comprehension" or within the "common knowledge" of "the average juror." Id., ¶29.

¶29 Burch argues that the Fitbit evidence was improperly admitted because the circuit court should have required expert testimony to establish the reliability of the science underlying Fitbit's technology. He notes that the Fitbit device features "a three-axis accelerometer sensor that generates data representing the user's movements," but explains that his "greater concern is with how the device processes the data into a meaningful output, how that output is exchanged with a phone or computer, and how that evidence ultimately ended up in Fitbit's business records."

¶30 In its written order rejecting Burch's argument that expert testimony was required, the circuit court explained that

Fitbit's step counters have been in the marketplace since 2009, and the "principle idea behind pedometers . . . for a significantly longer period than that." Many smartphones, the court added, "come equipped with a pedometer by default." Analogizing to a watch and a speedometer, the court noted that even though the average juror may not know "the exact mechanics" of a technology's "internal workings," the public may nevertheless "generally understand[] the principle of how it functions and accept[] its reliability." Similarly, the court reasoned, a Fitbit's use of sophisticated hardware and software does not render it an "unusually complex or esoteric" technology because the average juror is nevertheless familiar with what a Fitbit does and how it is operated.

¶31 This conclusion was reasonable and within the circuit court's discretionary authority. The circuit court correctly interpreted the standard for requiring expert testimony and reasonably applied that standard to the Fitbit evidence before it. Given the widespread availability of Fitbits and other similar wireless step-counting devices in today's consumer marketplace, the circuit court reasonably concluded Detrie's Fitbit was not so "unusually complex or esoteric" that the jury needed an expert to understand it.<sup>11</sup> The circuit court's

---

<sup>11</sup> To the extent Burch now argues that the Fitbit is outside the realm of lay comprehension because it is an "internet of things" device, we are unpersuaded. Wireless technology is nothing new. It is entirely within the "ordinary experience of mankind" to use a Bluetooth or Wi-Fi connection to transfer data from one device to another.

conclusion that expert testimony was not required under these circumstances was within the circuit court's discretion.<sup>12</sup>

## 2. Authentication

¶32 Wisconsin Stat. § 909.01 (2019-20)<sup>13</sup> sets out the evidentiary standard for authentication: "The requirements of authentication or identification as a condition precedent to admissibility are satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims." Simply put, authentication requires that a circuit court conclude, within its discretion, that the finder of fact could reasonably determine that the evidence sought to be admitted is what its proponent says it is. Id.; State v. Smith, 2005 WI 104, ¶¶31-33, 283 Wis. 2d 57, 699 N.W.2d 508. In this case, that means the State's authentication obligation is to present sufficient evidence to support a finding that the records produced by the State are in fact Fitbit's records associated with Detrie's Fitbit device.

¶33 Notably, Burch does not actually disagree that the State's records are accurate copies of Fitbit's records associated with Detrie's Fitbit device. Instead, he focuses his challenge on whether the State properly authenticated "the

---

<sup>12</sup> Of course, opposing counsel may attack the reliability of admitted evidence. T.A.T. v. R.E.B., 144 Wis. 2d 638, 652-53, 425 N.W.2d 404 (1988).

<sup>13</sup> All subsequent references to the Wisconsin Statutes are to the 2019-20 version unless otherwise indicated.

information within those records." Specifically, he argues that "the State failed to show that the Fitbit device reliably and accurately registered Detrie's steps that evening, and that that data was reliably and accurately transmitted to Fitbit's business records without manipulation."

¶34 Burch's argument reaches beyond the threshold question authentication presents. The circuit court's authentication obligation is simply to determine whether a fact-finder could reasonably conclude evidence is what its proponent claims it to be. Wis. Stat. § 909.01. The circuit court did so here by reviewing the Fitbit records and the affidavit of "a duly authorized custodian of Fitbit's records" averring that the records "are true and correct copies of Fitbit's customer data records," and then concluding the data was self-authenticating under Wis. Stat. § 909.02(12).<sup>14</sup> The circuit court's obligation is not to scrutinize every line of data within a given record and decide whether each line is an accurate representation of the facts. Rather, once the circuit court concludes the fact-finder could find that the records are what their proponent claims them to be, the credibility and weight ascribed to those

---

<sup>14</sup> More precisely, the circuit court held that the records were self-authenticating as certified records of regularly conducted activity. See Wis. Stat. § 909.02(12). Burch has not, either before the circuit court or this court, challenged the statements in the affidavit from Fitbit certifying that the records it provided are accurate copies of its records associated with Detrie's Fitbit device.

records are questions left to the finder of fact.<sup>15</sup> State v. Roberson, 2019 WI 102, ¶25, 389 Wis. 2d 190, 935 N.W.2d 813. The circuit court's conclusion that the Fitbit records were sufficiently authenticated therefore was within its discretion.

### III. CONCLUSION

¶35 Burch's appeal of his conviction for first-degree intentional homicide challenged the denial of two pre-trial evidentiary orders. We uphold both orders, and therefore affirm the judgment of conviction. Burch's cell phone data was properly admitted because, even if there was some constitutional defect in how it was obtained or retained, exclusion would be an improper remedy. The circuit court also permissibly exercised its discretion in admitting the Fitbit evidence; no expert was required and the State sufficiently authenticated the records from Fitbit.

*By the Court.*—The judgment of the circuit court is affirmed.

---

<sup>15</sup> Here, too, opposing counsel can attack the reliability of admitted evidence. See T.A.T., 144 Wis. 2d at 652-53.

¶36 REBECCA GRASSL BRADLEY, J. (*concurring*). I join the majority opinion in full. Because there are no controlling cases interpreting the Fourth Amendment to prohibit the second search of Burch's cellphone by the Brown County Sheriff's Office (Sheriff's Office), the exclusionary rule does not apply and suppression of the evidence obtained from that search would be improper.<sup>1</sup> I write separately to discuss the application of the Fourth Amendment to warrantless second searches of smartphones without consent.

¶37 Under the original meaning of the Fourth Amendment, law enforcement generally will need a warrant to search the contents of a smartphone, absent an exception to the warrant requirement. The consent-to-search exception, which the State argues authorized law enforcement to conduct a second search of Burch's smartphone data, does not extend to a second search of a smartphone by a different law enforcement agency investigating an entirely separate crime. "Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" Riley v. California, 573 U.S. 373, 403 (2014) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)). The Fourth Amendment secures "'the privacies of life' against 'arbitrary power,'" and embodies the "central aim of the Framers . . . 'to place obstacles in the way of a too permeating

---

<sup>1</sup> I also agree with the majority that the circuit court did not erroneously exercise its discretion by admitting evidence from Douglass Detrie's Fitbit device.

police surveillance.'" Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (quoted sources omitted).

¶38 The contents of smartphones constitute "papers" and "effects" secured by the Fourth Amendment, giving each of those categories their historical meanings and bearing in mind that "a cell phone search would typically expose to the government far more than the most exhaustive search of a house." Riley, 573 U.S. at 396. Accordingly, law enforcement generally must get a warrant before searching a cell phone. Id. at 403. Because Burch's consent to search covered only the Green Bay Police Department's initial search of his smartphone for evidence related to a hit-and-run investigation, a warrant should have been procured before the Sheriff's Office searched Burch's smartphone data as part of an unrelated murder investigation. Because neither this court nor the United States Supreme Court has decided this novel issue, the Sheriff's Office committed no misconduct in searching Burch's cell phone and the circuit court properly admitted the evidence obtained from the search. Accordingly, I respectfully concur.

## I

¶39 In June 2016, a few weeks after Nicole VanderHeyden's murder and the ensuing investigation by the Sheriff's Office, the Green Bay Police Department (Police Department) began investigating an entirely unrelated crime: an auto theft that resulted in a hit-and-run incident.<sup>2</sup> The stolen car belonged to Burch's roommate, and law enforcement identified Burch as a

---

<sup>2</sup> The vehicle was also lit on fire.

person of interest because he had last driven the car. Officer Robert Bourdelais of the Police Department interviewed Burch about the hit and run. Burch denied any involvement, but informed Officer Bourdelais that, on the night of the hit and run, he was texting a woman who lived one block away from the location of the accident. Burch stated that he did not go to the woman's house on the night of the incident, and never made arrangements to go to her house. According to Officer Bourdelais' testimony, he and Burch had the following exchange:

I asked him if I could see the text messages between him and [the woman], if my lieutenant and I could take a look at his text messages. He said that we could . . . . I [then] asked him if he would be willing to let me take his phone to this detective, download the information off the phone and then I'd bring the phone right back to him, probably take a half an hour and he said that would be fine.

¶40 The attorney eliciting Officer Bourdelais' testimony inquired: "When you asked [Burch] about downloading the information off of his phone, did you specifically limit the information to the text messages when you were talking to him?" Officer Bourdelais responded:

No, I didn't. Initially, when I had asked him, hey, do you mind if we take a look at those text messages, I refer to them as text messages because he said he was texting [the woman] back and forth, but from my experience as a police officer I know people communicate [by] phone calls, text messages, texting apps like WhatsApp, MINE, Facebook Messenger, things like that. So that's the information, I wanted information to corroborate that whatever conversation he had with [the woman] or communication he had supported his claims that he never went over to her house or made arrangements to go over to her house.

¶41 Following the exchange between Burch and Officer Bourdelais, Burch signed a consent form which read as follows: "I, George Stephen Burch, . . . voluntarily give Det. Danielski, Officer Bourdelais, or any assisting personnel permission to search my . . . Samsung cellphone." Subsequently, at the instruction of Officer Bourdelais, a Police Department forensic examiner downloaded all of the data from Burch's cellphone into the Police Department records database. The forensic examiner then converted the data into a readable format, and tabbed the data into categories such as text messages, images, and internet history. At the homicide trial, the forensic examiner testified that the Police Department retains smartphone data for an indefinite amount of time, noting that "[e]ver since [she] [has] been employed with [the Police Department], [they] have saved all extractions for long-term storage for as far back as [she] [has] been employed," which was roughly two years at the time of trial.

¶42 In August 2016 (two months after Burch consented to the search of his phone for the hit-and-run investigation), the Sheriff's Office identified Burch as a person of interest in the investigation into the murder of VanderHeyden based upon a DNA match on VanderHeyden's socks. Relying on databases shared between the Sheriff's Office and other local entities, detectives from the Sheriff's Office discovered that the Police Department had prior contact with Burch while investigating the unrelated hit-and-run incident. After the detectives learned that the Police Department had extracted all of Burch's

smartphone data in June 2016, they procured a copy of the data from the Police Department and searched its contents "for anything in the timeframe of the night of [the murder] into the [following] morning, whether it be calls, texts, internet history, any kind of location data available from that device." The detectives did not obtain a warrant for this search. In reviewing the data, the detectives discovered that, shortly after the murder, Burch repeatedly searched for news articles about the murder using his internet browser.

¶43 Additionally, during their warrantless search of the smartphone's contents, the detectives learned that Burch had a Google email account (Gmail). The detectives were aware that Gmail addresses are associated with a Google Dashboard, which tracks an individual's location based upon GPS, Wi-Fi, and cellphone tower data. The detectives procured a search warrant to obtain Google Dashboard information from Google. The location data placed Burch's smartphone at various critical places on the night of the murder, including the location of VanderHeyden's body and the on-ramp where her discarded clothing was discovered.

¶44 Burch was arrested and charged with first-degree intentional homicide. In a pre-trial motion, Burch moved to suppress the evidence obtained by the Sheriff's Office from the warrantless search of his smartphone data.<sup>3</sup> Burch argued that the Sheriff's Office "violated the Fourth Amendment when [it]

---

<sup>3</sup> Burch also filed a motion to exclude evidence related to Detrie's Fitbit device, which the circuit court denied.

searched the phone data initially seized by [the Police Department]." Specifically, Burch contended that the Sheriff's Office "blew past Mr. Burch's scope of consent, and likewise, obliterated any Fourth Amendment warrant exceptions." The circuit court denied Burch's suppression motion, and the State introduced at trial the evidence obtained from the smartphone. The jury convicted Burch of first-degree intentional homicide. Burch appealed the circuit court's decision to admit the evidence procured by the Sheriff's Office from its search of his smartphone data. The court of appeals certified Burch's Fourth Amendment challenge to this court, and we accepted certification.

## II

¶45 The Fourth Amendment provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. "The first clause outlaws promiscuous search and seizure, even as the second clarifies precisely what will be required for a particularized warrant to be valid." Laura K. Donohue, The Original Fourth Amendment, 83 U. Chi. L. Rev. 1181, 1193 (2016); State v. Pinder, 2018 WI 106, ¶¶48-51, 384 Wis. 2d 416, 919 N.W.2d 568. As understood at the time the Fourth Amendment was ratified, "[t]he government could not violate the right against search and seizure of one's person, house, papers, or effects absent either a felony arrest or a

warrant meeting the requirements detailed in the second clause." Donohue, supra, at 1193.

¶46 As the United States Supreme Court has repeatedly held, "the ultimate touchstone of the Fourth Amendment is 'reasonableness.'" Brigham City v. Stuart, 547 U.S. 398, 403 (2006). "[W]hether an individual has a reasonable expectation of privacy in avoiding the method of search and a reasonable expectation of privacy in the place searched are the questions that drive a court's examination of the reasonableness of the search." State v. Brereton, 2013 WI 17, ¶32, 345 Wis. 2d 563, 826 N.W.2d 369. "The general rule is that searches and seizures conducted without a warrant are not reasonable." State v. Randall, 2019 WI 80, ¶10, 387 Wis. 2d 744, 930 N.W.2d 223. However, there are a number of exceptions to the warrant requirement. See Riley, 573 U.S. at 382 ("In the absence of a warrant, a search is reasonable only if it falls within a specific exception to the warrant requirement."). "One of the exceptions to the warrant rule is that an individual's consent to search satisfies the constitutional 'reasonableness' requirement." Randall, 387 Wis. 2d 744, ¶10; see also Birchfield v. North Dakota, 136 S. Ct. 2160, 2185 (2016) ("It is well established that a search is reasonable when the subject consents[.]"). "If a search is premised on an individual's consent, it must cease immediately upon revocation of that consent," and an individual "may of course delimit as she chooses the scope of the search to which

she consents." Randall, 387 Wis. 2d 744, ¶10 (internal alterations and citations omitted).

¶47 Just a few years ago, the United States Supreme Court addressed the Fourth Amendment's application to a modern phenomenon: the proliferation of smartphones and their ever-increasing capacity to store mass amounts of data. The Court held that law enforcement generally must obtain a warrant before conducting a search of smartphone data. Specifically, the Riley Court clarified that "[its] holding . . . is not that the information on a cell phone is immune from search," but "instead that a warrant is generally required before such a search, even when a cell phone is seized incident to arrest."<sup>4</sup> Riley, 573 U.S. at 401. In reaching this holding, the Court recognized the "pervasiveness that characterizes cell phones" and how "[c]ell phones differ in both a quantitative and a qualitative sense from other objects." Id. at 393, 395. "The possible intrusion on privacy is not physically limited in the same way [as other objects] when it comes to cell phones." Id. at 394. "An internet search and browsing history, for example, can be found on an internet-enabled phone and could reveal an individual's private interests or concerns," and "historic location

---

<sup>4</sup> Although Riley involved the search-incident-to-arrest exception to the Fourth Amendment warrant requirement, the principles it espouses apply more broadly. See Riley v. California, 573 U.S. 373, 386 (2014) ("[O]fficers must generally secure a warrant before conducting such a search [of a cell phone]."); see also People v. Hughes, 958 N.W.2d 98, 108 (Mich. 2020) ("In Riley v. California, the Supreme Court of the United States held that officers must generally obtain a warrant before conducting a search of cell-phone data.").

information" could allow law enforcement to "reconstruct someone's specific movements down to the minute." Id. at 395-96.

¶48 The United States Supreme Court fully understood that its decision "[would] have an impact on the ability of law enforcement to combat crime." Id. at 401. After all, "[c]ell phones have become important tools in facilitating coordination and communication" for individuals committing crimes and "can provide valuable incriminating information about dangerous criminals." Id. But "[p]rivacy comes at a cost." Id. And the Fourth Amendment is designed to safeguard the people's security against unreasonable government intrusion. Riley recognizes that the Fourth Amendment safeguards this right by generally requiring law enforcement to procure a warrant before searching a smartphone.

¶49 A warrant requirement for searches of smartphone data comports with the original meaning of the Fourth Amendment. The Framers, "after consulting the lessons of history, designed our Constitution to place obstacles in the way of a too permeating police surveillance, which they seemed to think was a greater danger to a free people than the escape of some criminals from punishment." United States v. Di Re, 332 U.S. 581, 595 (1948). In particular, "the Fourth Amendment was the founding generation's response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity. Opposition to such searches was

in fact one of the driving forces behind the Revolution itself." Riley, 573 U.S. at 403. "Indeed, the character of that threat implicates the central concern underlying the Fourth Amendment—the concern about giving police officers unbridled discretion to rummage at will among a person's private effects." Arizona v. Gant, 556 U.S. 332, 345 (2009). For the Framers, it was absolutely necessary to ensure "the government not be allowed free rein to search for potential evidence of criminal wrongdoing." Donohue, supra, at 1194.

¶50 The Framers designed the Fourth Amendment to protect the people from government overreach. Described as the "very essence of constitutional liberty and security," the Fourth Amendment applies to "all invasions on the part of the government and its employes of the sanctity of a man's home and the privacies of life." Boyd, 116 U.S. at 630. "It is not the breaking of [one's] doors, and the rummaging of his drawers, that constitutes the . . . offense; but it is the invasion of his infeasible right of personal security, personal liberty, and private property[.]" Id. With this understanding in mind, "[t]he Supreme Court has . . . confirmed that the basic purpose of the Fourth Amendment 'is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials'"—that is, "to secure 'the privacies of life' against 'arbitrary power.'" Matthew DeVoy Jones, Cell Phones are Orwell's Telescreen: The Need for Fourth Amendment Protection in Real-Time Cell Phone Location Information, 67

Clev. St. L. Rev. 523, 533 (2019) (quoting Carpenter, 138 S. Ct. at 2213-14).

¶51 The Fourth Amendment specifically recognizes the right of people to be secure in their "persons, houses, papers, and effects." U.S. Const. amend. IV; see United States v. Jones, 565 U.S. 400, 406 (2012) ("[F]or most of our history the Fourth Amendment was understood to embody a particular concern for government trespass upon the areas ('persons, house, papers, and effects') it enumerates."). Much modern analysis of the Fourth Amendment has centered upon the primacy of protecting "houses." See Payton v. New York, 445 U.S. 573, 589 (1980) ("The Fourth Amendment protects the individual's privacy in a variety of settings. In none is the zone of privacy more clearly defined than when bounded by the unambiguous physical dimensions of an individual's home[.]"). However, as the Riley Court explained, smartphones implicate privacy interests more compelling than even those associated with the home. "A cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form[.]" Riley, 573 U.S. at 396-97.

¶52 Given the nature of its contents, a smartphone is not just another personal item; it is a device that holds many modern "privacies of life"—an area that receives acute and particularized protection from government interference under the

Fourth Amendment. See Boyd, 116 U.S. at 630. Governmental searches of smartphones invade "the indefeasible right of personal security, personal liberty, and private property," which Americans hold "sacred." Id. Permitting law enforcement to rummage through the data residing in smartphones without a warrant would "allow[] free rein to search for potential evidence of criminal wrongdoing," which the Fourth Amendment prohibits. With respect to smartphone data, as in the home, "all details are intimate details, because the entire area is held safe from prying government eyes." See Kyllo v. United States, 533 U.S. 27, 37 (2001).

¶53 The Fourth Amendment includes both "papers" and "effects" among the four enumerated categories protected from unreasonable searches. The contents of smartphones constitute "papers" within the original understanding of the Fourth Amendment. "Historically, private papers, including documents and pamphlets that challenged governmental power, served as a central point of contestation in the Founding era." Andrew Guthrie Ferguson, The "Smart" Fourth Amendment, 102 Cornell L. Rev. 547, 595-96 (2017). The Fourth Amendment's protection of "papers" "reflect[s] the importance of freedom of thought, expression, and communication." Id. According to Lord Camden in his seminal decision in Entick v. Carrington, "papers are often the dearest property a man can have." 19 How. St. Tr. 1029 (C.P. 1765).

¶54 The Framers' inclusion of "papers" within the protections of the Fourth Amendment was motivated in part by the

case of John Wilkes, "who was targeted for writing mocking articles about King George III" and had his papers seized by investigating officers. Ferguson, supra, at 596 (citation omitted). "The Wilkes controversy . . . directly influenced the [F]ramers of the Fourth Amendment. The English search and seizure cases received extensive publicity in England and in America, and the Wilkes case was the subject of as much notoriety and comment in the colonies as it was in Britain." Eric Schnapper, Unreasonable Searches and Seizures of Papers, 71 Va. L. Rev. 869, 912-13 (1985). "Wilkes' cause generated many supporters among American colonists, some of whom became key figures in the framing of the Constitution." Id. at 913. Based upon Wilkes' case, "[p]rotecting private papers . . . became a central rallying cry in the creation of constitutional liberty," receiving explicit protection under the United States Constitution. Ferguson, supra, at 596.

¶55 Today, the people's "papers" largely exist in digital form. "E-mails, texts, and other social media communication have replaced letter writing." Id. at 599. Additionally, calendars, notes, health information, photographs, restaurant and hotel reservations, airline flights, shopping and browsing histories, as well as banking transactions all reside in (or are accessible from) smartphones, forming a digital diary of one's life, accessible from a single source. Given the breadth and detail of this information, "individuals have expectations of privacy in their digital papers." Id. at 600. From the Framers' outrage over the search of Wilkes' papers to the

Court's concern regarding the search of David Riley's smartphone, the overarching aim "has always been the protection of ideas embodied in those papers"—not whether the papers are in physical or digital form. Id. at 613.

¶56 Some portion of the contents of smartphones, as well as the devices themselves, also constitute "effects," which "have historically been understood to mean personal property—the objects we possess." Id. at 578 (citing Dictionary Britannicum (Nathan Baily ed., 1730) (defining "effects" as "the goods of a merchant, tradesman") and Noah Webster, First Edition of an American Dictionary of the English Language (1828) (defining "effects" as "goods; moveables; personal estate")). "The early American understanding distinguished personal property from real property," and "personal property meant physical belongings"—items which were "obviously prized by the Founders" and accordingly received Fourth Amendment protection. Id. Founding-era history "demonstrates that effects were specifically included in the constitutional text [not only] because of the harms to privacy and dignity that could be incurred in their inspection, but also because of the risk of mishandling or damage generally associated with interferences with personal property." Maureen E. Brady, The Lost "Effects" of the Fourth Amendment: Giving Personal Property Due Protection, 125 Yale L.J. 946, 987 (2016). Founding-era sources suggest the Framers understood "[p]ersonal property [to] give[] its owner a right to exclude others from possessing, using, and interfering with the effect"—and most of all to "protect[]

privacy interests with respect to the property." Id. at 993-94 (discussing founding-era sources, including William Blackstone's Commentaries and Lord Camden's judgment in Entick v. Carrington).

¶57 Although "'effects' has captured rather less of the [United States] Supreme Court's attention" than "papers" and "houses," when the Court has addressed the topic, "property considerations loom large." Laura K. Donohue, The Fourth Amendment in a Digital World, 71 N.Y.U. Ann. Surv. Am. L. 553, 679 (2017). For example, in United States v. Jones, the United States Supreme Court held that law enforcement's installation of a GPS device on an individual's vehicle to monitor the vehicle's movements constituted a "search" under the Fourth Amendment, deeming it "beyond dispute" that a vehicle is an "effect" within the meaning of the Fourth Amendment. 565 U.S. 400, 404 (2012). The Court emphasized the government's "physical intrusion" of the "effect" at issue. Id. at 411. The Court did not focus on the physical attachment of the GPS device to the effect but rather the device's capture of sensitive and private information, "relay[ing] more than 2,000 pages of data over [a] 4-week period." Id. at 403; see also Ferguson, supra, at 606 ("[In Jones] the real harm was exposing the revealing personal data about the effect (car)."). That is, in Jones the Fourth Amendment analysis turned on the "capturing of data trails" of the owner and "invad[ing] the informational security of the effect." Ferguson, supra, at 606. The Court's reasoning in Jones applies no less to smartphones and the data they hold,

supporting the characterization of smartphones as "effects" entitled to constitutional protection from unreasonable searches and seizures.

### III

¶58 Having established a historical basis for the application of the Fourth Amendment's warrant requirement to smartphones and their data, it is necessary to address the application of the consent exception to the warrant requirement within the context of the facts of Burch's case. It is well-established that "[o]ne of the exceptions to the warrant rule is that an individual's consent to search satisfies the constitutional 'reasonableness' requirement." Randall, 387 Wis. 2d 744, ¶10; see also Birchfield, 136 S. Ct. at 2185. Burch gave consent for the Police Department to download and search his smartphone and its data as part of the investigation of the hit-and-run incident in June 2016. According to his testimony, Officer Bourdelais asked Burch if "[he] could see the text messages between him and [the woman]" on the night of the hit-and-run incident. Officer Bourdelais then asked Burch if he could "take his phone to this detective, download the information off the phone" and then bring it right back to Burch. Burch agreed to all requests in this exchange and signed a consent form saying he "voluntarily give[s] Det. Danielski, Officer Bourdelais, or any assisting personnel permission to search [his] . . . Samsung cellphone." Burch permitted Officer Bourdelais "or any assisting personnel" to download his smartphone's data and search for evidence of the hit-and-run

incident. Burch's consent encompassed the Police Department's investigation of a particular crime. The Constitution permitted this search. Schneckloth v. Bustamonte, 412 U.S. 218, 222 (1973) ("[A] search conducted pursuant to a valid consent is constitutionally permissible.").

¶59 Two months later, a different law enforcement agency—the Sheriff's Office—searched Burch's smartphone data while investigating an entirely separate crime. This search went beyond the scope of Burch's consent. Officer Bourdelais questioned Burch in June 2016 regarding the hit-and-run incident only, and obtained Burch's consent to download Burch's smartphone data "[to] corroborate that whatever conversation [Burch] had with [the woman] . . . supported his claims that he never went over to her house" the night of the hit and run. The consent form did not include any language authorizing a second search by a separate law enforcement agency for a different crime. The form authorized only Officer Bourdelais, the forensic examiner (Det. Danielski), and their assisting personnel to view the smartphone's contents. Any search beyond the scope of Burch's consent would require a warrant.

¶60 The State argues that this court's decision in State v. Betterley, 191 Wis. 2d 406, 529 N.W.2d 216 (1995), allows law enforcement to take a "second look" at smartphone data that was previously searched. That case does not apply to searches of cell phone data. In Betterley, officers at the St. Croix County Jail seized a ring from the defendant during an inventory search. Id. at 414. Later that day, a New Richmond police

officer asked to see the ring, believing it was evidence that the defendant had committed insurance fraud. Id. at 415. The New Richmond police officer retained the ring as evidence without obtaining a warrant. Id. This court held that "the permissible extent of the second look [at evidence] is defined by what the police could have lawfully done without violating the defendant's reasonable expectations of privacy during the first search, even if they did not do it at that time." Id. at 418. Because the defendant had a diminished expectation in privacy in the ring after forfeiting it during the first search, the second look at the ring was permissible, so long as it was "no more intrusive" than the first search. Id.

¶61 Betterley does not apply to cell phone data retrieved pursuant to the owner's consent. Betterley involved an inventory search of an item, not the consent-to-search exception to the warrant requirement. Unlike searches conducted with consent, inventory searches are "administrative by nature, not an investigation motivated by a search for evidence." State v. Weber, 163 Wis. 2d 116, 132, 471 N.W.2d 187 (1991). More importantly, physical items such as rings are qualitatively different than searches of smartphone data. Examination of a ring reveals nothing more than the physically observable item itself, while smartphones contain—and conceal—the "privacies of life," which generally are not viewable by others at a glance. For this reason, smartphones "differ in both a quantitative and a qualitative sense from other objects." Riley, 573 U.S. at 393. "[I]t is no exaggeration to say that

many of the more than 90% of American adults who own a cell phone keep on their person a digital record of nearly every aspect of their lives—from the mundane to the intimate. Allowing the police to scrutinize such records on a routine basis is quite different from allowing them to search a personal item or two in the occasional case." Id. at 395. Certainly, "the possible intrusion on privacy is not physically limited in the same way [as other objects] when it comes to cell phones." Id. at 394. Accordingly, Betterley does not inform the Fourth Amendment analysis governing searches of cell phone data.

¶62 Even if "a Fourth Amendment violation has occurred," however, it "does not mean the exclusionary rule applies," particularly because "exclusion [of evidence] is the last resort." State v. Dearborn, 2010 WI 84, ¶35, 327 Wis. 2d 252, 786 N.W.2d 97. "To trigger the exclusionary rule, police misconduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." Id., ¶36 (quoted source omitted). For the reasons stated in the majority opinion, there was no misconduct by the Sheriff's Office. Neither this court nor the United States Supreme Court has declared that second searches of cell phone data by separate law enforcement agencies require a warrant. Accordingly, suppression of the evidence obtained during the Sheriff's Office's second search would be inappropriate and I respectfully concur.

\* \* \*

¶63 "The great end, for which men entered into society, was to secure their property." Entick v. Carrington, 19 How. St. Tr. 1029 (C.P. 1765) (Lord Camden presiding). "Property must be secured, or liberty cannot exist." Discourses on Davila, in 6 The Works of John Adams 280 (C. Adams ed. 1851). "The Fourth Amendment imposes limits on search-and-seizure powers in order to prevent arbitrary and oppressive interference by enforcement officials with the privacy and personal security of individuals." United States v. Martinez-Fuerte, 428 U.S. 543, 554 (1976). Because smartphones contain the "privacies of life," law enforcement generally needs a warrant to search the data they hold unless an exception to the warrant requirement applies.

¶64 REBECCA FRANK DALLET, J. (*concurring in part, dissenting in part*). Under the Fourth Amendment, when the police want to search a person's private information, they generally need a warrant. The Brown County Sheriff's Office searched George Steven Burch's private cell phone data without obtaining a warrant, assuming that Burch's consent for another agency to download his phone's data for a wholly separate investigation obviated its Fourth Amendment duty to do so. It did not. The Sheriff's Office's warrantless search of Burch's cell phone data violated the Fourth Amendment, and the evidence obtained from that unlawful search should be suppressed. The majority opinion's contrary holding ignores the novel constitutional problems presented by private cell phone information, is inconsistent with the Fourth Amendment's text, and undermines the exclusionary remedy for Fourth Amendment violations. I therefore respectfully dissent from that part of the majority opinion.<sup>1</sup>

#### I. BACKGROUND

¶65 A Green Bay Police Department (GBPD) officer interviewed Burch while investigating crimes involving the car Burch would borrow for work. Burch denied his involvement but acknowledged that he was text messaging a friend that night who lived near the scene. When the officer asked Burch if he and his lieutenant could see those text messages, Burch verbally consented. After the officer explained that it was easier to

---

<sup>1</sup> I join Parts I. and II.B. of the majority opinion because I agree that the circuit court permissibly admitted evidence regarding a Fitbit device.

download "the information" from the phone than to take screenshots, Burch verbally consented to allowing the officer to take his phone to a GBPD detective for that purpose.<sup>2</sup> The officer then presented Burch with a standardized written consent form. The form contained the heading "City of Green Bay Police Department" and indicated that Burch "voluntarily" gave a named GBPD officer, a named GBPD detective, as well as any "assisting personnel," "permission to search" his "Samsung Cellphone." Burch signed the form. The officer testified that he requested only "text messages, phone calls, Facebook posts, and photographs taken any time after 11:00 p.m." the night of the accident; yet, to access that information, the GBPD downloaded the entire contents of Burch's phone.

¶66 Two months later, the Sheriff's Office was investigating a homicide that had occurred a few weeks before the crimes being investigated by the GBPD. It matched Burch's DNA to DNA collected from the victim's body, her socks, and a cord believed to be used in her murder. The Sheriff's Office

---

<sup>2</sup> At trial, the officer testified that by "the information," he meant any communications between Burch and his friend that would corroborate Burch's alibi:

Initially, when I had asked [Burch], hey, do you mind if we take a look at those text messages, I refer to them as text messages because he said he was texting [his friend] back and forth, but from my experience as a police officer I know people communicate phone calls, text messages, texting apps like WhatsApp, MINE, Facebook Messenger, things like that. So that's the information, I wanted information to corroborate that whatever conversation he had with [his friend] or communication he had supported his claims that he never went over to [the victim's] house or made arrangements to go over to her house.

also discovered that the GBPD had retained the full data extraction from Burch's cell phone. After reviewing the GBPD's files and seeing Burch's signed consent form, the Sheriff's Office searched that data without first obtaining a warrant. The search led the Sheriff's Office to Burch's internet search history and his Google email account. The internet history revealed that Burch had viewed online stories about the victim's disappearance 64 times. The email account allowed the Sheriff's Office to issue Google a subpoena for Burch's Google Dashboard records, which included his location data from the night of the murder. The location data placed Burch's cell phone near the victim's residence and the field where her body was discovered around the time of the victim's death.

## II. ANALYSIS

¶67 The Fourth Amendment inquiry here is two-fold. The first consideration is whether the Sheriff's Office's warrantless search of the GBPD's download of Burch's data was unreasonable. If so, it violated the Fourth Amendment, and the question becomes whether excluding the unlawfully obtained evidence would sufficiently deter the same police conduct in the future. These questions involve a mixed standard of review, under which we uphold the circuit court's findings of historical fact unless they are clearly erroneous, but we review de novo the application of constitutional principles to those facts. See State v. Blackman, 2017 WI 77, ¶25, 377 Wis. 2d 339, 898 N.W.2d 774.

A. The Sheriff's Office's Warrantless Search Was Unreasonable.

¶68 The Fourth Amendment to the United States Constitution prohibits the government from conducting "unreasonable" searches of a person, a person's home, or her "effects":

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause . . . .

The Amendment seeks to secure "the privacies of life" against such unreasonable searches by placing "obstacles in the way of a too permeating police surveillance." See Carpenter v. United States, 585 U.S. \_\_\_, 138 S. Ct. 2206, 2214 (2018). Police surveillance amounts to a "search," for purposes of the Fourth Amendment, when it collects information in which the person has a reasonable expectation of privacy. E.g., id. at 2213-14.

¶69 To protect one's reasonable expectation of privacy, the text of the Fourth Amendment communicates a "strong preference for searches conducted pursuant to a warrant." See Illinois v. Gates, 462 U.S. 213, 236 (1983); U.S. Const. amnd. IV. Indeed, a warrantless search is per se unreasonable, see Schneckloth v. Bustamonte, 412 U.S. 218, 219 (1973), and presumptively violates the Fourth Amendment, see State v. Tate, 2014 WI 89, ¶27, 357 Wis. 2d 172, 849 N.W.2d 798. That presumption is overcome only when the warrantless search falls under one of the "few specifically established and well-delineated exceptions." State v. Coffee, 2020 WI 53, ¶24, 391 Wis. 2d 831, 943 N.W.2d 845.

¶70 Consent is one such exception. State v. Hogan, 2015 WI 76, ¶55, 364 Wis. 2d 167, 868 N.W.2d 124. As with any

exception to the warrant requirement, consent is "jealously and carefully drawn," and must be "confined in scope" and "strictly circumscribed." See Jones v. United States, 357 U.S. 493, 499 (1958); Terry v. Ohio, 392 U.S. 1, 25-26, 29 (1968). Consent to a particular search must therefore be "unequivocal and specific." State v. Reed, 2018 WI 109, ¶8, 384 Wis. 2d 469, 920 N.W.2d 56. Even absent express limits, the scope of consent is neither "boundless" nor "perpetual." See State v. Douglas, 123 Wis. 2d 13, 21-22, 365 N.W.2d 580 (1985) (lead opinion). Rather, its scope is determined objectively as "the typical reasonable person [would] have understood" it from "the exchange between the officer and the suspect." Florida v. Jimeno, 500 U.S. 248, 251 (1991). When the police rely on consent as their justification for not getting a warrant, the State carries the burden to demonstrate by clear and convincing evidence that the search remained within the scope of that consent. See Reed, 384 Wis. 2d 469, ¶58; Douglas, 123 Wis. 2d at 22 (explaining that a warrantless search exceeding the scope of consent is unreasonable).

¶71 The lawfulness of the Sheriff's Office's search therefore turns on two sub-questions: (1) although he consented to specific GBPD personnel downloading his cell phone information, did Burch maintain a reasonable expectation of privacy in that information such that the Sheriff's Office review of it was a Fourth Amendment search; and, if so, (2) did the Sheriff's Office act unreasonably by searching the GBPD's download of Burch's cell phone data without a warrant, in light of Burch's consent to the GBPD?

1. Burch Maintained a Reasonable Expectation of Privacy in the GBPD's Download of His Cell Phone Data.

¶72 In the Fourth Amendment context, the United States Supreme Court has clearly expressed that cell phone data is in an evidence class of its own because it "implicate[s] privacy concerns far beyond those implicated by the search of" other physical belongings. Riley v. California, 573 U.S. 373, 393 (2014). Cell phones are unique in that they are almost always with us and they store "vast quantities of personal information." Id. at 386. Thus, by carrying cell phones, people carry with them "a digital record of nearly every aspect of their lives—from the mundane to the intimate." Id. at 395. That digital record may include a person's internet "search and browsing history" and "[h]istoric location information," see id. at 395-96, allowing someone with access to that information to "generate[] a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations," see United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring). Although traditionally most private information was kept in one's home, advances in digital technology have shifted that paradigm such that searching a personal cell phone "would typically expose to the government far more than the most exhaustive search of a house." Riley, 573 U.S. at 396-97. Accordingly, people have a unique and heightened expectation of privacy in their cell phone data that demands commensurate Fourth Amendment protection. See id. at 386, 393; People v. Hughes, 958 N.W.2d 98, 112 (Mich. 2020)

("Riley distinguished cell-phone data from other items . . . in terms of the privacy interests at stake.").

¶73 The unique privacy expectation in cell phone data informs why Burch's consent to the GBPD does not relieve the Sheriff's Office of its obligation to get a warrant for its own review. Burch's consent, as "the typical reasonable person [would] have understood" it, had the "expressed object" of the GBPD reviewing messages to verify his alibi for the GBPD's investigation. See Jimeno, 500 U.S. at 251. The GBPD officer's report explained that Burch "consented to Lt. Allen and I [two GBPD officers] looking at the text messages between him and [Burch's acquaintance] last night and also indicated I could take his phone to the department to have the information on it downloaded." Burch's signed consent form is also specific to the "City of Green Bay Police Department" and indicated that Burch gave certain members of the GBPD permission to search his phone. Critically absent from the report or the consent form is any mention of any other law enforcement agency, the possibility of the GBPD sharing the entirety of the downloaded data, or even that Burch was consenting to the GBPD retaining indefinitely all of his phone's information. Cf. Douglas, 123 Wis. 2d at 21-22.

¶74 Burch's consent was therefore limited to the GBPD for the GBPD's investigation.<sup>3</sup> See Terry, 392 U.S. at 25-26, 29 (requiring courts to interpret warrant exceptions as "confined in scope" and "strictly circumscribed"). With respect to other agencies and their investigations, Burch maintained a reasonable expectation of privacy in the data downloaded by the GBPD but unrelated to its investigation, including his internet search history and Google email account. See Carpenter, 138 S. Ct. at 2217 (holding that, because of cell phone data's "unique nature," a person "maintains a legitimate expectation of privacy" in the data even after consensually giving it to another party for a limited purpose); Hughes, 958 N.W.2d at 111 (concluding that the lawful seizure and search of certain cell phone information does not "extinguish[] that otherwise reasonable expectation of privacy in the entirety" of that information). Consequently, the Sheriff's Office's subsequent review of Burch's data invaded Burch's reasonable expectation of privacy such that it was a search under the Fourth Amendment.

2. The Sheriff's Office Acted Unreasonably in Searching the GBPD's Download of Burch's Cell Phone Data.

¶75 The Sheriff's Office decided that no warrant was required for its search after determining that Burch's consent

---

<sup>3</sup> The circuit court's determination that Burch placed no parameters on the scope of his consent is suspect given that his conversation with the GBPD about his phone was strictly limited to his text messages. The categorical uniqueness of private cell phone data requires circuit courts to take seriously the admonition that exceptions to the warrant requirement like consent be interpreted as "confined in scope" and "strictly circumscribed." See Riley v. California, 573 U.S. 373, 382, 393 (2014); Terry v. Ohio, 392 U.S. 1, 25-26, 29 (1968).

to the GBPD extended to the Sheriff's Office. But as discussed above, Burch's "unequivocal and specific" consent extended only to certain members of the GBPD, and only so they could review his text messages to confirm his alibi. See Reed, 384 Wis. 2d 469, ¶8. Burch did not consent to all of the information on his phone being available to other law enforcement agencies for some later, unrelated investigation. And the Sheriff's Office did not independently get Burch's consent to search his cell phone information.

¶76 Given those facts, no reasonable person in Burch's position would have understood that his consent to the GBPD was an open invitation for any other law enforcement agency to search his private information whenever it wanted to and without a warrant. Therefore, the consent exception to the Fourth Amendment's warrant requirement does not apply to the Sheriff's Office's subsequent warrantless search of Burch's private cell phone data for an unrelated investigation. That search was unreasonable and violated the Fourth Amendment.

B. Evidence of Burch's Google Location Data and His Internet Search History Should Be Suppressed.

¶77 Having concluded that the Sheriff's Office's search violated the Fourth Amendment, the next question is whether the exclusionary rule applies; that is, whether excluding, or suppressing, the unlawfully obtained evidence would sufficiently deter the same police conduct in the future. Here, Burch's Google location data and his internet search history should be excluded because if they are not, other law enforcement agencies are likely to repeat the Sheriff's Office's unconstitutional

search of downloaded cell phone data, especially given the ubiquity of cell phones and the increasing prevalence of personal digital data in criminal investigations.

¶78 The exclusionary rule—that evidence obtained in violation of the Fourth Amendment be excluded from trial—ensures that the Fourth Amendment's right to be free from unreasonable searches remains one "of substance rather than mere tinsel." Hoyer v. State, 180 Wis. 407, 415, 193 N.W. 89 (1923). By excluding otherwise relevant evidence, "[t]he exclusionary rule generally serves to 'deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence.'" Blackman, 377 Wis. 2d 339, ¶68 (quoting Herring v. United States, 555 U.S. 135, 150-51 (2009)). The rule thus incentivizes "the law enforcement profession as a whole" to conduct itself "in accord with the Fourth Amendment." Gates, 462 U.S. at 261 n.15 (White, J., concurring in the judgment).

¶79 Given that critical function, the United States Supreme Court has permitted deviation from the exclusionary rule only when the deterrent value of excluding the evidence is "marginal" or "nonexistent" and outweighed by the social cost of doing so. See, e.g., United States v. Leon, 468 U.S. 897, 913-17, 922 (1984). Such is the case when there is no police misconduct to deter or when the police misconduct is "isolated," "nonrecurring," and "attenuated." See id. at 922; Herring, 555 U.S. at 137, 144. For example, excluding unlawfully obtained evidence is inappropriate if the police acted in objectively reasonable reliance on either a facially

valid warrant properly issued by a neutral, detached magistrate; an apparently constitutional statute; or a binding appellate precedent. See Leon, 468 U.S. 897 (warrants);<sup>4</sup> Illinois v. Krull, 480 U.S. 340 (1987) (statutes); Davis v. United States, 564 U.S. 229, 239-41 (2011) (appellate precedents). Likewise, exclusion is inappropriate when an arresting officer acts in objectively reasonable reliance on either a judicial or police employees' infrequent clerical mistake. See Arizona v. Evans, 514 U.S. 1, 14-16 (1995) (court clerk made a recordkeeping error regarding outstanding arrest warrants only once "every three or four years"); Herring, 555 U.S. at 144-47 (police employees' clerical error in warrant database had never happened before). The common thread through each of these cases is that the fault lies with someone who is not directly engaged in the "competitive enterprise of ferreting out crime"; who has "no stake in the outcome of particular prosecutions." See Evans, 514 U.S. at 15.

¶80 Conversely, the exclusionary rule applies when evidence is unlawfully obtained due to an error made by law enforcement. See Leon, 468 U.S. at 923. For instance, evidence should be suppressed when law enforcement secures evidence based on a facially deficient warrant, or when a warrant is issued based on an officer knowingly or recklessly stating a falsehood in the warrant affidavit. See id. The same goes for when police exceed a valid warrant's authority when executing it. See id. As for the police relying on statutory authority, the

---

<sup>4</sup> See also Massachusetts v. Sheppard, 468 U.S. 981, 988-91 (1984).

exclusionary rule still applies when police officers misinterpret and "act outside the scope" of a statute and when a reasonable officer would have known either that the law in question is unconstitutional or that the conduct authorized by the statute violates other clearly established law. Krull, 480 U.S. at 355, 360 n.17. Indeed, the rule applies even to unlawfully negligent police conduct when the conduct is "recurring or systemic." E.g., Herring, 555 U.S. at 144.

¶81 The exclusionary rule applies in this case because it was the Sheriff's Office's conduct that rendered unlawful its search of Burch's cell phone, not some detached third party's. There was no statute or judicial precedent condoning a warrantless search of another agency's download of a person's private cell phone data. Instead, the Sheriff's Office judged for itself, incorrectly, that the Fourth Amendment's warrant requirement did not apply to Burch's cell phone data. The unlawful conduct here—not obtaining a warrant to search Burch's private cell phone data—is solely attributable to the Sheriff's Office's detectives. And because those detectives are directly engaged in the "competitive enterprise of ferreting out crime," the exclusionary rule should apply. See Evans, 514 U.S. at 15.

¶82 Applying the rule is also justified because the record demonstrates that warrantless searches of private cell phone information are commonplace, and therefore likely to recur. Officers from both the GBPD and the Sheriff's Office confirmed that it is "very common" for agencies to share "full downloads" of private cell phones with other agencies without first obtaining a warrant, adding that their agencies "regularly" do

so. This widespread neglect of the Fourth Amendment's warrant requirement is just the kind of "systemic negligence" the exclusionary rule is designed to correct. See Herring, 555 U.S. at 144. The exclusionary rule thus squarely applies here.

¶83 The State's counterarguments are unavailing. Its contention that the Sheriff's Office reasonably relied upon its own determination regarding the scope of Burch's consent misses the point. It is not up to the police to determine the contours of an exception to a constitutional requirement restricting their own conduct. See Leon, 468 U.S. at 959 (Brennan, J., dissenting) (presciently lamenting that exceptions to the exclusionary rule would not stay "confined" but instead be wrongfully extended "to situations in which the police have conducted a warrantless search solely on the basis of their own judgment"). Moreover, because the police may encounter circumstances that are on the margins of the law regarding warrant exceptions—as is the case here—police officers are required to "err on the side of constitutional behavior" and get a warrant.<sup>5</sup> See United States v. Johnson, 457 U.S. 537, 561

---

<sup>5</sup> The State erroneously argues that the Sheriff's Office's search is akin to law enforcement's ability to take a "second look" at physical evidence inventoried during a jail intake or that it already lawfully seized. See State v. Betterley, 191 Wis. 2d 406, 418, 529 N.W.2d 216 (1995); State v. Riedel, 2003 WI App 18, ¶16, 259 Wis. 2d 921, 656 N.W.2d 789. But as the United States Supreme Court explained in Riley, "cell phones, as a category, implicate privacy concerns far beyond those implicated" by physical objects. 573 U.S. at 393. And because a "search of the information on a cell phone bears little resemblance" to other types of searches, the rationales for other searches do not extend to cell phone information. See id. at 386. Therefore, the State's arguments fail. See People v. Hughes, 958 N.W.2d 98, 111-15 (Mich. 2020).

(1982); Blackman, 377 Wis. 2d 339, ¶53 (warrantless searches executed outside any "clearly delineated" warrant exception are "per se unreasonable" and "unlawful"). The Sheriff's Office's erroneous determination that Burch's consent extended to the Sheriff's Office is no justification for failing to get a warrant.

¶84 Nor is the Sheriff's Office relieved of its Fourth Amendment duty to get a warrant simply because law enforcement agencies "regularly" share this type of information. The pervasiveness of this practice is no defense to the exclusionary rule; it is the reason to apply it. See Herring, 555 U.S. at 144 (exclusion applies when unreasonable police conduct is "recurring" or "systemic"). The same goes for the majority's characterization of the Sheriff's Office's conduct as "by the book." Majority op., ¶22. If following "the book" leads to violations of the Fourth Amendment, then the exclusionary rule's deterrent value is at its peak. Excluding evidence obtained by following such an unlawful and widespread policy provides significant societal value by both specifically deterring continued adherence to an unconstitutional practice and more broadly incentivizing police agencies to adopt policies in line with the Fourth Amendment.<sup>6</sup> See Wayne R. LaFave, 1 Search & Seizure § 1.3(i) (6th ed. 2020). This is especially true when

---

<sup>6</sup> The State counters that because the Sheriff's Office may have had access to Burch's Google email account and internet search history via a lawful, independent source, that evidence should not be excluded. See State v. Carroll, 2010 WI 8, ¶¶44-45, 322 Wis. 2d 299, 778 N.W.2d 1. But the State has forfeited that argument by failing to raise it below. See State v. Counihan, 2020 WI 12, ¶25, 390 Wis. 2d 172, 938 N.W.2d 530.

the Constitution already provides law enforcement with a simple solution for how to lawfully obtain cell phone data: get a warrant. See Riley, 573 U.S. at 403.

C. The Majority Opinion Has No Support in Fourth Amendment Jurisprudence.

¶85 The majority opinion offers a contrary analysis that ignores the novel constitutional problems presented by cell phone data, is inconsistent with the Fourth Amendment's text, and undermines the exclusionary remedy.

¶86 The majority opinion's analysis reveals a lack of appreciation for the fundamental differences between digital cell phone data and more "traditional," non-digital evidence that law enforcement might share with other agencies. The Fourth Amendment treats cell phone data differently because it often contains nearly all the "privacies of [a person's] life," such that "any extension" of Fourth Amendment principles "to digital data has to rest on its own bottom." See Riley, 573 U.S. at 393, 403 (quoting another source); Carpenter, 138 S. Ct. at 2219 (explaining that Fourth Amendment jurisprudence must account for the "seismic shifts in digital technology"). Accordingly, it is a grave analytical error to "mechanically apply[]" to cell phone data Fourth Amendment rationales that were developed without such invasive technologies in mind. Carpenter, 138 S. Ct. at 2219; see also Riley, 573 U.S. at 400-01 (rejecting the argument that the police can search cell phone data under the same rationale that allows them to obtain "the same information from a pre-digital counterpart"). Or, as the United States Supreme Court put it, treating cell

phone data the same as its non-digital analogues "is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together." Riley, 573 U.S. at 393. The majority opinion, however, is content to toss a saddle on a spaceship and call it a horse. Nowhere does the majority opinion account for Burch's special privacy interest in his cell phone data, leaving a tremendous hole in its exclusionary rule analysis.

¶87 More troubling is the majority's disregard for the Fourth Amendment's text. It is bedrock Fourth Amendment law that search warrants are generally required and that a search without a warrant is per se unlawful. See, e.g., City of Ontario v. Quon, 560 U.S. 746, 760 (2010); Blackman, 377 Wis. 2d 339, ¶53. The majority's assertion that "there is nothing concerning under current Fourth Amendment doctrine with how the Sheriff's Office detectives conducted themselves" shockingly discards this well-settled principle. Indeed, the majority opinion fails to even mention the presumption that warrantless searches violate the Fourth Amendment.

¶88 But worse than mere silence, the majority's refusal to apply the exclusionary rule flips this presumption on its head. According to the majority, if "no case from this court or the federal courts" directs the police to get a warrant, then the police act "reasonably" in not getting a warrant. Majority op., ¶23. The majority appears to create a new prerequisite for applying the exclusionary rule, holding that it applies only if a court has previously declared that the police conduct at issue

is unconstitutional. Imposing this hurdle undermines the exclusionary remedy for Fourth Amendment violations and is directly contrary to both our and the United States Supreme Court's Fourth Amendment jurisprudence.

¶89 All of which makes inexcusable the majority opinion's refusal to address the constitutionality of the Sheriff's Office's search. Despite law enforcement's admittedly "very common" practice of sharing with other agencies entire downloads of private cell phone data, that recurring Fourth Amendment violation will continue with impunity unless and until the court engages with the specific Fourth Amendment issue raised by private cell phone information. By skipping straight to whether the exclusionary rule applies, the majority opinion deprives aggrieved defendants—and future courts—of the very prior precedent now necessary to remedy law enforcement's continued unconstitutional conduct:

Forgoing a knotty constitutional inquiry makes for easier sledding, no doubt. But the inexorable result is "constitutional stagnation"—fewer courts establishing law at all, much less clearly doing so, . . . [creating a] Catch-22. [Defendants] must produce precedent even as fewer courts are producing precedent. Important constitutional questions go unanswered precisely because no one's answered them before. Courts then rely on that judicial silence to conclude there's no equivalent case law on the books. . . . If courts leapfrog the underlying constitutional merits in cases raising novel issues like digital privacy, then constitutional clarity—matter-of-fact guidance about what the Constitution requires—remains exasperatingly elusive. Result: gauzy constitutional guardrails as technological innovation outpaces legal adaptation.

Zadeh v. Robinson, 928 F.3d 457, 479-80 (5th Cir. 2019) (Willet, J., concurring), cert. denied, 141 S. Ct. 110 (2020).

Together with its new prior-precedent requirement, the majority opinion's avoidance of the Fourth Amendment issues here perpetuates a cycle of diminished police accountability and courts' unwillingness to address it.

¶90 Given that the Fourth Amendment law specific to cell phone data is undeveloped, this court should be providing "clear guidance to law enforcement through categorical rules." Riley, 573 U.S. at 398; see also Michigan v. Summers, 452 U.S. 692, 705 n.19 (1981) (explaining that clear "workable" rules are necessary so that difficult Fourth Amendment questions are not resolved in an "ad hoc, case-by-case fashion by individual police officers") (quoting another source)). If a law enforcement agency wishes to search a person's private information, such as cell phone data, and the person did not consent to that agency's search, the agency must get a warrant.

### III. CONCLUSION

¶91 The Sheriff's Office should have obtained a warrant to search Burch's private cell phone data. Because it did not, the evidence it found as a result of that search should be suppressed. The majority's refusal to apply the exclusionary rule is incompatible with our Fourth Amendment jurisprudence and perverts the long-standing bedrock requirement that police obtain a warrant to search private information. I therefore respectfully dissent from that part of the majority opinion.

¶92 I am authorized to state that Justice JILL J. KAROFKY joins this opinion and that Justice ANN WALSH BRADLEY joins this opinion except for footnote 1.



¶93 ANN WALSH BRADLEY, J. (*dissenting*). Ubiquitous use does not mean the average wearer of a Fitbit knows how it works. Nor does ubiquitous use indicate reliability sufficient to be admissible in a court of law.

¶94 An average jury member would likely know what a Fitbit is and what it does. Of course, as relevant here, it counts the wearer's steps. But that isn't the question. In determining whether expert testimony is required, the relevant inquiry is how a Fitbit counts the wearer's steps and then ultimately, whether it does so with sufficient reliability.

¶95 How does it work? A Fitbit device uses a microelectronic triaxial accelerometer to capture a person's body motion in three-dimensional space and record related data. This motion data is then analyzed by utilizing proprietary algorithms to surmise patterns and thus to identify daily steps taken.

¶96 Is it sufficiently reliable to be admitted as evidence in court? I don't know. But, I do know that the answer does not lie in its ubiquitous use.

¶97 I also know that absent expert testimony there is insufficient foundation in this record for the majority to determine, in essence, that a presumption of accuracy and reliability attends the underlying technology of a Fitbit. The error of such a presumption is made manifest by reference to an overarching analysis of 67 studies on Fitbit accuracy disseminated by the National Center for Biotechnology Information (NCBI), under the auspices of the U.S. National

Institutes of Health (NIH). The researchers found that Fitbit devices were "likely to meet acceptable accuracy for step count approximately half the time." Lynne M. Feehan, et al., Accuracy of Fitbit Devices: Systematic Review and Narrative Syntheses of Quantitative Data, <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6107736/> (2018).

¶98 In citing this study, I neither endorse nor disclaim its conclusions. It suggests, however, when a compilation of studies indicates acceptable accuracy is met only "half the time," that something may be amiss with the majority's presumption of accuracy and reliability.

¶99 Expert testimony is required when matters are presented that are "unusually complex." White v. Leeder, 149 Wis. 2d 948, 960, 440 N.W.2d 557 (1989). Movement measured by a "microelectronic triaxial accelerometer" and analyzed by proprietary algorithms certainly fits that bill.

¶100 In my view, the technology underlying a Fitbit is not within the ordinary experience of an average jury member. Fitbits and other wearable devices may be ubiquitous, but it does not follow from this premise that the technology underlying their use is not "unusually complex."

¶101 Expert testimony assists the trier of fact to understand the evidence and to determine a fact in issue. The accuracy of the number of steps recorded on Douglass Detrie's Fitbit is certainly a fact in issue. Thus, expert testimony should have been required to assist the jury in understanding the technology and assessing its reliability.

¶102 Invoking a deferential standard, it is not unusual for an appellate court to do only a cursory analysis of an evidentiary issue. But this is not the usual case and a more nuanced analysis is required.

¶103 This case presents a groundbreaking question. To my knowledge, this is the first appellate court decision in the country to conclude that Fitbit step-counting evidence is admissible absent expert testimony explaining how the device works. The parties have not cited, and I have not found, any case making such a proclamation. The majority's analysis provides a slim reed upon which to support such a novel determination.

¶104 Rather than allowing evaluation of the question, the majority cuts off the debate. It essentially rubber stamps the circuit court's erroneous analysis and declares Fitbit's technology to be simple enough to be presented as evidence without the benefit of an expert witness or further consideration of its reliability.

¶105 Although I join Justice Dallet's dissent, concluding that the search of Burch's cell phone at issue violated his Fourth Amendment rights and that the good faith exception to the warrant requirement does not apply, I do not join footnote 1 that concurs with the majority's analysis of the Fitbit evidence. Because I conclude that the circuit court erroneously admitted the Fitbit evidence without an expert witness to establish the reliability of the science underlying the Fitbit technology, I respectfully dissent.

## I

¶106 I briefly recount the facts that are relevant to the issue on which I write: the admission of the Fitbit evidence.

¶107 As the majority opinion sets forth, the initial suspect in the crime at issue here was Douglass Detrie, the victim's boyfriend. Majority op., ¶4. However, the investigation shifted after police learned that Detrie's Fitbit device had recorded only 12 steps during the time the homicide was committed. Burch was ultimately arrested and charged.

¶108 The State sought to present evidence regarding Detrie's Fitbit, and Burch moved to exclude it. Id., ¶11. As relevant here, Burch contended that the State must present expert testimony to establish the reliability of the science behind the Fitbit device. Id.<sup>1</sup>

¶109 The circuit court granted Burch's motion in part and denied it in part. Specifically, the circuit court excluded Fitbit evidence related to sleep monitoring, but it allowed the admission of the step-counting data without the testimony of an expert regarding the science underlying the Fitbit technology. Id., ¶11 & n.3.

¶110 In the circuit court's estimation, a Fitbit is more akin to an electronic monitoring device (which does not require expert testimony, see State v. Kandutsch, 2011 WI 78, 336

---

<sup>1</sup> Burch made several additional arguments, including an assertion that Fitbit's records were not properly authenticated, which he renews on appeal. Because I determine that expert testimony was necessary to admit the evidence in question, I do not reach Burch's arguments regarding authentication.

Wis. 2d 478, 799 N.W.2d 865) than to a preliminary breath test (which requires expert testimony, see State v. Doerr, 229 Wis. 2d 616, 599 N.W.2d 897 (Ct. App. 1999)). Similarly, the circuit court distinguished Fitbit data from DNA, fingerprint analysis, blood alcohol content tests, tool mark evidence and accident reconstruction because "few people encounter those things in their everyday life."

¶111 Comparing a Fitbit to an electronic monitoring device, the circuit court stated that a Fitbit is "passively worn by a person," and the device collects data "based on that person's movements, which is then transmitted and recorded. There is no active manipulation by the wearer to achieve the results; the results are simply a record of the wearer's movements, i.e., their location or the number of steps they took." Thus, in the circuit court's view "the step-counting feature of the Fitbit Flex, like the [electronic monitoring device], is not so unusually complex or esoteric that the jury will require the aid of expert testimony to interpret the information."

¶112 At trial, because it was not required to provide an expert to introduce the data from Detrie's Fitbit, the State relied upon the testimony of Tyler Behling, a computer forensic crime analyst with the Brown County Sheriff's Office. Although Behling claimed to have knowledge of how a Fitbit works "on a high level," he did not know the answer when asked how a Fitbit and a Bluetooth device send information from one to the other, how Fitbit stores its data, whether Fitbit data can be edited,

whether the device would register steps while it is not being worn, or what a Fitbit's error rate is.

¶113 Despite the dearth of technical testimony regarding how a Fitbit actually works, the majority now affirms the circuit court's determination. It concludes that "[g]iven the widespread availability of Fitbits and other similar wireless step-counting devices in today's consumer marketplace, the circuit court reasonably concluded Detrie's Fitbit was not so 'unusually complex or esoteric' that the jury needed an expert to understand it." Majority op., ¶31.

## II

¶114 It has long been the law that expert testimony is required when a matter involves "special knowledge or skill or experience on subjects which are not within the realm of the ordinary experience of mankind, and which require special learning, study and experience." Cramer v. Theda Clark Mem'l Hosp., 45 Wis. 2d 147, 150, 172 N.W.2d 427 (1969). "The requirement of expert testimony is an extraordinary one," and should be applied "only when unusually complex or esoteric issues are before the jury." White, 149 Wis. 2d at 960.

¶115 "In considering what constitutes the 'ordinary experience of mankind'—i.e. the average juror—courts have not tailored this standard to the lowest common denominator. Rather, courts attempt to evaluate, on a case-by-case basis, whether expert testimony is required because the issue is outside the realm of lay comprehension." Kandutsch, 336 Wis. 2d 478, ¶29.

¶116 The circuit court here determined that the technology underlying a Fitbit is not outside the realm of lay comprehension. It compared a Fitbit to a watch in that "the public generally understands the principle of how it functions and accepts its reliability without knowing the exact mechanics of its internal workings." Further, it determined that a Fitbit is not subject to "active manipulation by the wearer to achieve the results; the results are simply a record of the wearer's movements, i.e., their location or the number of steps they took."

¶117 But the expert testimony standards do not rest on ubiquity. Instead, they rest on the complexity of the subject matter. Although many members of the jury may have been wearing Fitbits or similar devices, such a fact would not inform the question of whether those jury members understand how a Fitbit works or whether the technology is reliable.

¶118 What does the average person really know about how a Fitbit works, much less its reliability? As one study described it, "Fitbit devices use a microelectronic triaxial accelerometer to capture body motion in 3-dimensional space, with these motion data analyzed using proprietary algorithms to identify patterns of motion to identify daily steps taken, energy expenditure, sleep, distance covered, and time spent in different intensity of activities." Feehan, et al., supra. According to the majority, the average juror would understand, without expert

testimony, not only what a "microelectronic triaxial accelerometer" is, but how it works. Really?<sup>2</sup>

¶119 If the State had presented an expert, that expert would have had to meet the requirements for expert testimony established by the United States Supreme Court in Daubert.<sup>3</sup> Pursuant to the Daubert standard, as codified in Wis. Stat. § 907.02(1),<sup>4</sup> the circuit court must act as a gatekeeper and make a threshold determination that the testimony is reliable in order for it to be presented at trial. State v. Dobbs, 2020 WI 64, ¶43, 392 Wis. 2d 505, 945 N.W.2d 609. By not requiring the State to present an expert, the circuit court and the majority allow the State to skirt this initial reliability determination.

¶120 There are various ways in which threshold reliability can be demonstrated. See 7 Daniel D. Blinka, Wisconsin Practice Series: Wisconsin Evidence § 702.402 (4th ed. 2020). There may

---

<sup>2</sup> Further, the intricacies of Fitbit's technology are "proprietary," setting up an additional roadblock to the jury's full knowledge and full understanding of how the device works. See State v. Loomis, 2016 WI 68, ¶66, 371 Wis. 2d 235, 881 N.W.2d 749 (explaining that "proprietary nature" has been invoked to prevent disclosure of certain information).

<sup>3</sup> Daubert v. Merrell Dow Pharm., Inc., 509 U.S. 579 (1993).

<sup>4</sup> Wisconsin Stat. § 907.02(1) provides:

If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if the testimony is based upon sufficient facts or data, the testimony is the product of reliable principles and methods, and the witness has applied the principles and methods reliably to the facts of the case.

be a statute indicating that certain tests or methods are admissible. See, e.g., Wis. Stat. § 885.235 (addressing chemical tests for intoxication). There is no statute addressing Fitbit evidence.

¶121 We can also look to court precedent which has already determined certain principles to be reliable. See, e.g., State v. Hanson, 85 Wis. 2d 233, 244, 270 N.W.2d 212 (1978) (discussing the reliability of the underlying principles of speed radar detection that employs the Doppler effect). The reliability of Fitbit's step counting capability is a novel issue, so there is no precedent on point.

¶122 Stipulations or judicial notice may also be appropriate when a fact is "capable of accurate and ready determination by resort to sources whose accuracy cannot reasonably be questioned." Wis. Stat. § 902.01(2)(b). Again, these do not fit the present scenario—the reason we are here is because the parties do not agree and Burch reasonably questions the accuracy of Fitbit's step count.

¶123 Finally, if none of the above proves to be an acceptable avenue to demonstrate the accuracy and reliability of the scientific principles sufficient to be accorded a prima facie presumption, expert testimony is necessary to explain the underlying scientific principles and to demonstrate their reliability. Here, no expert was presented.

¶124 The evidentiary process requires that the scientific principles be presented to the court before the evidence is determined to be reliable. In a court of law, process matters.

Without fulfilling one of these avenues, the threshold reliability determination cannot be made.

¶125 And what of Fitbit's reliability? Such reliability can depend on a number of factors, such as whether the user has self-manipulated the data, if the Fitbit is temporarily removed, where on the body the device is worn, or the type of physical activity in which the wearer is engaged. Feehan, et al., supra; Katherine E. Vinez, The Admissibility of Data Collected from Wearable Devices, 4 Stetson J. Advoc. & L. 1, 16 (2017). In a comprehensive aggregation of 67 different studies, researchers found that "[c]onsistent evidence indicated that Fitbit devices were likely to meet acceptable accuracy for step count approximately half the time." Feehan, et al., supra. Yet in the view of the majority and of the circuit court, an expert is not necessary to establish the reliability of Detrie's step count—the Fitbit evidence can go before the jury with no technical or scientific explanation.

¶126 Indeed, questions arise about the reliability of wearable devices despite their widespread acceptance. See Vinez, supra, at 16. If reliability questions exist, where better than the circuit court to present the case for and against such reliability? Instead of remanding to the circuit court for evaluation of the question, the majority curtly

declares Fitbit's technology to be simple enough to be put before a jury without the benefit of an expert.<sup>5</sup>

¶127 When new and popular devices emerge, courts should be wary of blindly accepting the data they produce without a thorough examination of the underlying technology. "Machines warrant no blind faith, and whatever trust they receive must be earned through the crucible of the rules of evidence." Brian Sites, Machines Ascendant: Robots and the Rules of Evidence, 3 Geo. L. Tech. Rev. 1, 1-2 (2018). In many cases, such an examination will require an expert. In my view, this is such a case.

¶128 Rather than break new ground as does the majority, I would proceed with caution. Basing the necessity of expert testimony on ubiquity rather than complexity sets a dangerous path.

¶129 For the foregoing reasons, I respectfully dissent.

---

<sup>5</sup> See Nicole Chauriye, Wearable Devices as Admissible Evidence: Technology is Killing our Opportunities to Lie, 24 Cath. U. J. L. & Tech. 495, 517 (2016) (arguing that "the trier of fact would greatly benefit from mandated expert testimony to explain the accuracy and details of the data recorded by the wearable technology").



The court is not  
filing this document  
at this time  
Received  
D. Peal  
2-24-20

1 Jennifer Granick, Bar No. 168423  
2 ACLU Foundation  
3 39 Drumm Street  
4 San Francisco, CA 94111  
5 415-343-0758  
6 jgranick@aclu.org

7 Jacob A. Snow, Bar No. 270988  
8 ACLU Foundation of Northern California  
9 39 Drumm Street  
10 San Francisco, CA 94111  
11 415-621-2493  
12 jsnow@aclunc.org

13 Peter Bibring, Bar No. 223981  
14 Mohammad Tajsar, Bar No. 280152  
15 ACLU Foundation of Southern California  
16 1313 West 8<sup>th</sup> Street  
17 Los Angeles, CA 90017  
18 213-977-5295  
19 pbibring@aclusocal.org  
20 mtajsar@aclusocal.org

21 *On the brief:*  
22 Brett Max Kaufman  
23 Alexia Ramirez  
24 Nathan Freed Wessler  
25 ACLU Foundation  
26 125 Broad Street, 18th Floor  
27 New York, NY 10004  
28 212-549-2500  
bkaufman@aclu.org  
aramirez@aclu.org  
nwessler@aclu.org

*Attorneys for Amici Curiae American Civil Liberties Union and American Civil Liberties Union of Northern and Southern California in Support of Petitioner*

**SUPERIOR COURT OF THE STATE OF CALIFORNIA  
FOR THE COUNTY OF LOS ANGELES**

Case No. 20CCPC0020

IN RE SEARCH WARRANT TO GOOGLE  
FOR ALL RECORDS ASSOCIATED WITH  
GOOGLE ACCOUNT  
SCOTTARCLA@GMAIL.COM

**[PROPOSED] BRIEF OF AMICI  
CURIAE ACLU, ACLU OF SOUTHERN  
CALIFORNIA, AND ACLU OF  
NORTHERN CALIFORNIA IN  
SUPPORT OF MOTION TO QUASH  
SEARCH WARRANT**

[PROPOSED] BRIEF OF AMICI CURIAE ACLU, ACLU OF SOUTHERN CALIFORNIA, AND ACLU OF  
NORTHERN CALIFORNIA IN SUPPORT OF MOTION TO QUASH SEARCH WARRANT  
CASE No. 20CCPC0020

1 **TABLE OF CONTENTS**

2 TABLE OF AUTHORITIES ..... iv

3 INTRODUCTION ..... 2

4 ARGUMENT ..... 3

5 I. Online Email And Storage Accounts Like Mr. Budnick’s Contain Vast Amounts

6 Of Extremely Sensitive, Private Information..... 3

7 II. Warrants For Digital Data Must Be Scrupulously Particular and Narrow in Scope

8 In Order To Be Constitutional. .... 5

9 A. The Fourth Amendment Requires That Warrants Clearly Limit What

10 Officers May Seize, And That Searches Are Designed Only To Find

11 Relevant Information. .... 6

12 B. Overbreadth And Particularity Are Especially Important When Officers

13 Seek Access to Digital Information. .... 8

14 III. Courts Can Craft Warrants To Constrain Invasive Rummaging—A Risk With

15 Even Seemingly Limited Descriptions of Information. .... 9

16 A. Seizures should be limited to relevant categories of information. .... 10

17 B. Seizures should be limited by time frame and other available

18 characteristics..... 11

19 C. Searches Must Be Limited By Probable Cause, And Should Use Clean

20 Teams, Data Deletion, And Other Tools To Protect Privacy. .... 12

21 IV. The Warrant for Mr. Budnick’s Google Account Violates CalECPA, and

22 Everything Provided In Response Should Be Destroyed. .... 17

23 A. CalECPA Provides Strong, Clear Digital Privacy Rules For Government,

24 Companies, And The Public. .... 17

25 B. The Search Warrant Failed to Comply with CalECPA. .... 18

26 1. The Warrant to Mr. Budnick Violates CalECPA’s Particularity

27 Requirement. .... 19

28

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

2. Mr. Budnick May Not Have Received Notice Required by  
CalECPA..... 20

C. Because This Warrant Violated CalECPA, All Materials Officers  
Obtained Pursuant to the Warrant Must Be Destroyed..... 22

CONCLUSION..... 22

1 **TABLE OF AUTHORITIES**

2 **Cases**

3 *Aday v. Superior Court,*  
55 Cal.2d 789 (1961) ..... 7, 8

4 *Andresen v. Maryland,*  
5 427 U.S. 463 (1976)..... 6

6 *Berger v. New York,*  
7 388 U.S. 41 (1967)..... 6, 9

8 *Burrows v. Superior Court,*  
9 13 Cal. 3d 238 (1974) ..... 7

10 *Carpenter v. United States,*  
11 138 S. Ct. 2206 (2018)..... 1, 4, 5, 9

12 *Carroll v. United States,*  
13 267 U.S. 132 (1925)..... 9

14 *Doe v. Prosecutor,*  
566 F. Supp. 2d 862 (S.D. Ind. 2008) ..... 17

15 *Fazaga v. FBI,*  
16 916 F.3d 1202 (9th Cir. 2019) ..... 15

17 *Groh v. Ramirez,*  
18 540 U.S. 551 (2004)..... 6

19 *Horton v. California,*  
20 496 U.S. 128 (1990)..... 8

21 *In re [REDACTED]@gmail.com,*  
62 F. Supp. 3d 1100 (N.D. Cal. 2014) ..... 12, 16

22 *In re Search of Google Email Accounts identified in Attachment A,*  
23 92 F. Supp. 3d 944 (D. Alaska 2015) ..... 12

24 *In re Search of Info. Associated With Four Redacted Gmail Accounts,*  
25 371 F. Supp. 3d 843 (D. Or. 2018) ..... 12

26 *In re Search Warrant,*  
27 71 A.3d 1158 (Vt. 2012)..... 13, 16

1     *Johnson v. United States*,  
        333 U.S. 10 (1948)..... 17

2

3     *Kentucky v. King*,  
        563 U.S. 452 (2011)..... 6

4

5     *Kyllo v. United States*,  
        533 U.S. 27 (2001)..... 9

6

7     *Marron v. United States*,  
        275 U.S. 192 (1927)..... 6

8

9     *Maryland v. Garrison*,  
        480 U.S. 79 (1987)..... 7

10    *Maurer v. Pitchess*,  
        691 F.2d 434 (9th Cir. 1982) ..... 15

11

12    *People v. Chapman*,  
        36 Cal.3d 98 (1984) ..... 19

13

14    *People v. Frank*,  
        38 Ca. 3d 711 (1985) ..... 6

15

16    *People v. Kraft*,  
        23 Cal.4th 978 (2000) ..... 6

17

18    *Riley v. California*,  
        573 U.S. 373 (2014)..... 4

19

20    *Saunders v. Superior Court*,  
        12 Cal. App. 5th Supp. 1 (Cal. App. Dep’t Super. Ct. 2017) ..... 22

21

22    *Stanford v. Texas*,  
        379 U.S. 476 (1965)..... 2, 6

23

24    *United States v. Abboud*,  
        438 F.3d 554 (6th Cir. 2006) ..... 11

25

26    *United States v. Cardwell*,  
        680 F.2d 75 (9th Cir. 1982) ..... 6

27

28    *United States v. Comprehensive Drug Testing, Inc. (CDT)*,  
        621 F.3d 1162 (9th Cir. 2010) ..... 8, 10, 13, 15

1 *United States v. Diaz*,  
841 F.2d 1 (1st Cir. 1988)..... 11

2

3 *United States v. Diggs*,  
544 F.2d 116 (3d Cir. 1976) ..... 17

4

5 *United States v. Drebin*,  
557 F.2d 1316 (9th Cir. 1977) ..... 7

6

7 *United States v. Griffith*,  
867 F.3d 1265 (D.C. Cir. 2017)..... 12

8

9 *United States v. Hill*,  
459 F.3d 966 (9th Cir. 2006) ..... 6, 13

10

11 *United States v. Hillyard*,  
677 F.2d 1336 (9th Cir. 1982) ..... 7

12

13 *United States v. Jones*,  
565 U.S. 400 (2012)..... 9

14

15 *United States v. Kow*,  
58 F.3d 423 (9th Cir. 1995) ..... 7

16

17 *United States v. Morgan*,  
743 F.2d 1158 (6th Cir. 1984) ..... 17

18

19 *United States v. Payton*,  
573 F.3d 859 (9th Cir. 2009) ..... 4

20

21 *United States v. Shipp*, 392 F. Supp. 3d 300 (E.D.N.Y. 2019)..... 4, 10, 11, 15

22

23 *United States v. Stabile*,  
633 F.3d 219 (3d Cir. 2011) ..... 14

24

25 *United States v. Stetkiw*  
No. 18-20579, 2019 WL 2866516 (E.D. Mich. July 3, 2019)..... 16

26

27 *United States v. Stubbs*,  
873 F.2d 210 (9th Cir. 1989) ..... 7

28

*United States v. Warshak*,  
631 F.3d 266 (6th Cir. 2010) ..... 1

*United States v. Wey*,  
256 F. Supp. 3d 355 (S.D.N.Y. 2017) ..... 11

1 *United States v. Williams*,  
2 592 F.3d 511 (4th Cir. 2010) ..... 14

3 **Statutes**

4 18 USC § 2703..... 21

5 Cal. Penal Code § 1546.1(a) ..... 17

6 Cal. Penal Code § 1546.1(d)..... 18, 19, 20

7 Cal. Penal Code § 1546.2(a) ..... 18, 21

8 Cal. Penal Code § 1546.2(b)..... 18, 21

9 Cal. Penal Code § 1546.4(a) ..... 18, 22

10 Cal. Penal Code § 1546.4(c) ..... 18, 22

11 **Other Authorities**

12 *About Google One*, Google..... 4

13 *About Google Photos*, Google ..... 12

14 Bill Analysis, Assembly Committee on Appropriations, SB 178 (May 28, 2015)..... 21

15 Bill Analysis, Assembly Committee on Privacy and Consumer Protection, SB 178 (June 23,  
16 2015) ..... 19

17 Bill Analysis, Assembly Committee on Public Safety, SB 178 (July 14, 2015) ..... 20

18 Bill Analysis, Privacy: Electronic Communications: Search Warrants, Senate Committee on  
19 Appropriations, SB 178 (April 22, 2015) ..... 21

20 *BlackBag Announces Release of BlackLight 2019 R2*, BlackBag (Sept. 5, 2019) ..... 15

21 Emily Berman, *Digital Searches, the Fourth Amendment, and the Magistrates’ Revolt*, 68  
22 Emory L.J. 49 (2018)..... 16

23 Karen Kent et al., *Guide to Integrating Forensic Techniques Into Incident Response:*  
24 *Recommendations of the National Institute of Standards and Technology*, No. 800-86,  
25 U.S. Dep’t of Commerce (Aug. 2006)..... 14

26 *Metadata: Piecing Together a Privacy Solution*, ACLU of N. Cal. (2014) ..... 17

27

28

1           The American Civil Liberties Union (“ACLU”) is a nationwide, nonprofit, nonpartisan  
2 organization dedicated to the principles of liberty and equality embodied in the Constitution and  
3 our nation’s civil rights laws. Since its founding in 1920, the ACLU has frequently appeared  
4 before the Supreme Court and other federal courts in numerous cases implicating Americans’  
5 right to privacy in the digital age, including as counsel in *Carpenter v. United States*, 138 S. Ct.  
6 2206 (2018), and as amicus in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

7           The ACLU of Southern California and the ACLU of Northern California (“ACLU of  
8 Northern and Southern California”) are two California state affiliates of the national ACLU. The  
9 ACLU of Northern and Southern California participate in a statewide Technology and Civil  
10 Liberties Project, founded in 2004, which works specifically on legal and policy issues at the  
11 intersection of new technology and privacy, free speech, and other civil liberties and civil rights.  
12 The ACLU of Northern and Southern California supported the passage of CalECPA and served  
13 as key advisors to the law's authors, Senators Mark Leno and Joel Anderson, throughout the  
14 legislative process. Accordingly, amici are uniquely positioned to provide the Court with a  
15 comprehensive perspective on the purpose and meaning of CalECPA.<sup>1</sup>

16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  

---

27 <sup>1</sup> Amici would like to thank Jacob Apkon and Thomas McBrien, students in the Technology Law  
28 & Policy Clinic at NYU School of Law, for their significant contributions to this brief.

## INTRODUCTION

1  
2 The Founders may not have foreseen the advanced technologies of the digital age, but  
3 they drafted the Fourth Amendment to forbid warrants like the one at issue in this proceeding.  
4 The central motivation behind the ratification of the Fourth Amendment was to ensure that  
5 government officials could not invade the privacies of a person’s life without justification,  
6 restraint, and oversight. The amendment rejected the “general warrant,” an imperial legal  
7 instrument granting the government unrestrained authority to rummage through people’s lives  
8 under cover of governmental power.

9 The warrant that Sergeant Richard Biddle obtained for Scott Budnick’s Google account  
10 data is a vast departure from what the Fourth Amendment permits. Officer Biddle sought every  
11 scrap of information in Mr. Budnick’s account from the account’s inception. A legal demand to  
12 seize all the paper records someone had created over the years would be an impermissible  
13 general warrant, forbidden by the Fourth Amendment and reviled by the framers. *Stanford v.*  
14 *Texas*, 379 U.S. 476, 482–83 (1965) (describing warrants that “authorized . . . the arrest and  
15 seizure of all the papers of a named person thought to be connected with a libel” as a type of  
16 general warrant). Today, such court orders are even more pernicious. Americans in 1792 did not  
17 generate anything close to the volume of information that ordinary people today store on phones,  
18 computers, and in the “cloud.”

19 The astounding amount of digital information subject to seizure and search presents  
20 serious challenges for privacy. Seizure of the contents of an entire online account can reveal an  
21 astonishingly complete record of an individual’s life—private papers, reading lists, appointment  
22 books, correspondence, photographs, location history, research interests, and more. In many  
23 cases, even seizures that appear at first glance to be narrowly framed would give police huge  
24 quantities of irrelevant and private information. But courts have the necessary tools to ensure that  
25 warrants for electronic information are not general warrants, either on their face or in effect.

26 First, courts must limit “intentional over-seizures.” Warrants to third parties such as Google or  
27 Facebook should be cabined to only relevant categories of data for a defined time period, as  
28 supported by probable cause. The warrant in this matter utterly failed that test. Second, even

1 when investigators must over-seize electronic data for pragmatic reasons, warrant-issuing courts  
2 can and should require officers to conduct searches in a manner designed to uncover relevant  
3 evidence and avoid rummaging through irrelevant personal matters. Courts could impose search  
4 protocols, or require officers to document their searches to ensure an opportunity for effective  
5 judicial oversight. With modern forensic tools, there is no need for law enforcement officers to  
6 randomly open files on a hard drive. Searches can target relevant actors, keywords, or time  
7 frames so as not to be overbroad. Courts could require “clean teams” or special masters to  
8 segregate relevant from irrelevant information, or require the government to forego application  
9 of the plain view doctrine so as not to take advantage of overbroad searches. The goals of these  
10 limitations are fundamental to the Fourth Amendment: to cabin law enforcement discretion,  
11 prevent searches from straying beyond their justifications, protect privacy, and limit the risk of  
12 abuse. And when violations of the Fourth Amendment occur, as in this case, expungement of  
13 improperly seized or searched information is a necessary and proper remedy.

14 While the Fourth Amendment requires quashal here, Officer Biddle’s warrant is also an  
15 egregious violation of the California Electronic Communications Privacy Act (“CalECPA”).  
16 That law, which took effect in January of 2016, established clear statutory protections for  
17 Californians’ privacy rights when a government entity seeks electronic communications and  
18 device information. Those protections include concrete particularity requirements and a  
19 requirement that the government notify the target. The government met neither requirement here.  
20 When the government obtains information in violation of CalECPA, the statute also provides a  
21 remedy: suppression of evidence in court and destruction of material unlawfully obtained. Any  
22 of Mr. Budnick’s information that Officer Biddle obtained from Google should, under CalECPA,  
23 be promptly destroyed.

## 24 ARGUMENT

### 25 I. Online Email And Storage Accounts Like Mr. Budnick’s Contain Vast Amounts 26 Of Extremely Sensitive, Private Information.

27 Digital information generated by today’s devices and services reveals individuals’ private  
28 matters far beyond what one could learn from physical analogs. *See Riley v. California*, 573 U.S.  
[PROPOSED] BRIEF OF AMICI CURIAE ACLU, ACLU OF SOUTHERN CALIFORNIA, AND ACLU OF  
NORTHERN CALIFORNIA IN SUPPORT OF MOTION TO QUASH SEARCH WARRANT  
CASE No. 20CCPC0020

1 373, 394 (2014). A device the size of a human palm can store practically unlimited quantities of  
2 data. *Id.* For example, sixteen gigabytes of information—the standard capacity of a smart phone  
3 several years ago—“translates to millions of pages of text, thousands of pictures, or hundreds of  
4 videos.” *Id.* Google offers 15 gigabytes of data storage for free, and up to 200 gigabytes of  
5 storage at negligible cost. *See About Google One*, Google, <https://one.google.com/about>.  
6 Google’s servers store volumes of data, including email, photos, videos, calendar items,  
7 documents and spreadsheets, videos watched, search terms entered, websites visited, and the  
8 locations users have been to while carrying their phones. These accounts contain people’s most  
9 intimate and private documents—love notes, tax records, business plans, health data, religious  
10 and political affiliations, personal finances, and digital diaries, to name just a few. Today, people  
11 who carry cell phones, use social media, or take advantage of online storage generate an almost  
12 incomprehensible quantity of sensitive and private information. A search of even one such  
13 account is deeply invasive. *See United States v. Payton*, 573 F.3d 859, 861–62 (9th Cir. 2009)  
14 (“There is no question that computers are capable of storing immense amounts of information  
15 and often contain a great deal of private information. Searches of computers therefore often  
16 involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches  
17 of other containers.”). Police access to social media accounts and online communications  
18 services present a “threat [that] is further elevated . . . because, perhaps more than any other  
19 location—including a residence, a computer hard drive, or a car—[they] provide[] a single  
20 window through which almost every detail of a person’s life is visible.” *United States v. Shipp*,  
21 392 F. Supp. 3d 300, 308 (E.D.N.Y. 2019) (describing Facebook).

22         Moreover, while our garages and desk drawers may fill up with knickknacks, requiring  
23 periodic spring cleaning, digital data can pile up and persist indefinitely, meaning law  
24 enforcement is capable of accessing years’—and soon, decades’—worth of personal information.  
25 *See Carpenter v. United States*, 138 S. Ct. 2206, 2218 (2018); *Riley*, 573 U.S. at 394. This  
26 combination of volume, depth and longevity of personal information raises strong privacy  
27 concerns because in aggregate, digital information reveals much more than the sum of each part.  
28 *See Riley*, 573 U.S. at 394.

1 A warrant like the one at issue here could also subject individuals like Mr. Budnick to  
2 abuse and harassment. Casual police access to the incredible variety and volume of personal  
3 correspondence and other private information stored in the cloud today could be used to deter  
4 lawful political advocacy, or to scare others who wish to engage in advocacy for other issues.  
5 Passwords and PIN codes, which the warrant demanded, could be used to spy on account  
6 holders, allowing officers access to digital information without judicial oversight. Passwords  
7 could also be misused to send fake messages, impersonating the account holder. Location  
8 information can reveal personal relationships, religious affiliation, political activity, and health  
9 conditions. Stock holdings and financial data could only be of prurient interest under  
10 circumstances like those involved in this case.

11 The staggeringly broad categories of information Officer Biddle sought, and appears to  
12 have obtained, from Mr. Budnick’s Google account go far beyond what is constitutionally  
13 permissible. Officer Biddle asked for categories of information that could not have possibly  
14 contained any evidence of the so-called “conspiracy” he was investigating (e.g., *all* images and  
15 videos, location history, search history, play store applications, credit card numbers, securities  
16 records, and other financial data). As *amici* explain below, Officer Biddle’s warrant would  
17 violate the Fourth Amendment even if there were probable cause of criminal activity, which  
18 there is not.

19 **II. Warrants For Digital Data Must Be Scrupulously Particular and Narrow in**  
20 **Scope In Order To Be Constitutional.**

21 The Fourth Amendment is intended “to place obstacles in the way of a too permeating  
22 police surveillance.”<sup>2</sup> *Carpenter*, 138 S. Ct. at 2214 (citation and quotation marks omitted). It  
23 requires that search warrants particularly describe the places to be searched and the things to be  
24 seized (particularity), and prohibits search for or seizure of anything for which there is not  
25 probable cause (overbreadth). To protect the highly private and sensitive nature of today’s

26 \_\_\_\_\_  
27 <sup>2</sup> California Electronic Privacy Act (“CalECPA”), Cal. Penal Code § 1546.1(e) (2017)  
28 guarantees Mr. Budnick independent legal rights that were violated in the course of Officer  
Biddle’s investigation. *See infra* Part IV.

1 electronically stored information, warrants must impose strict restrictions on law enforcement’s  
2 electronic searches and seizures so as to avoid unnecessary exposure of our intimate details to  
3 investigators.

4 **A. The Fourth Amendment Requires That Warrants Clearly Limit What**  
5 **Officers May Seize, And That Searches Are Designed Only To Find Relevant**  
6 **Information.**

7 The Fourth Amendment protects against general warrants, which were “the worst  
8 instrument of arbitrary power . . . that ever was found in an English law book.” *Stanford*, 379  
9 U.S. at 481 (quoting founding father James Otis). Search warrants must be particular and narrow  
10 in scope. *See, e.g., id.* at 485 (“The requirement that warrants shall particularly describe the  
11 things to be seized makes general searches under them impossible and prevents the seizure of  
12 one thing under a warrant describing another.”); *Berger v. New York*, 388 U.S. 41, 58 (1967)  
13 (“The Fourth Amendment’s requirement that a warrant ‘particularly describ(e) the place to be  
14 searched, and the persons or things to be seized,’ repudiated these general warrants and ‘makes  
15 general searches . . . impossible and prevents the seizure of one thing under a warrant describing  
16 another.’” (alteration in original)); *Groh v. Ramirez*, 540 U.S. 551, 557 (2004) (“[T]he  
17 warrant . . . was deficient in particularity because it provided no description of the type of  
18 evidence sought.”); *Kentucky v. King*, 563 U.S. 452, 459 (2011) (“a warrant may not be issued  
19 unless probable cause is properly established and the scope of the authorized search is set out  
20 with particularity.”); *People v. Kraft*, 23 Cal.4th 978, 1041 (2000) (citing *Andresen v. Maryland*,  
21 427 U.S. 463, 480 (1976)).

22 “Specificity has two aspects: particularity and breadth. Particularity is the requirement  
23 that the warrant must clearly state what is sought. Breadth deals with the requirement that the  
24 scope of the warrant be limited by the probable cause on which the warrant is based.” *United*  
25 *States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006) (citations omitted). A warrant is sufficiently  
26 particularized only if “nothing is left to the discretion of the officer executing the warrant.”  
27 *Marron v. United States*, 275 U.S. 192, 196 (1927); *see also United States v. Cardwell*, 680 F.2d  
28 75 (9th Cir. 1982); *People v. Frank*, 38 Ca. 3d 711, 724 (1985) (The particularity requirement is  
[PROPOSED] BRIEF OF AMICI CURIAE ACLU, ACLU OF SOUTHERN CALIFORNIA, AND ACLU OF  
NORTHERN CALIFORNIA IN SUPPORT OF MOTION TO QUASH SEARCH WARRANT  
CASE No. 20CCPC0020

1 met “if the warrant imposes a meaningful restriction upon the objects to be seized.”). The  
2 warrant must also constrain invasive “fishing expeditions” by authorizing searches only for  
3 evidence of a crime for which there is probable cause. *See Maryland v. Garrison*, 480 U.S. 79,  
4 84 (1987).

5 A search is unlawfully general where the accompanying warrant “left to the executing  
6 officers,” rather than to the magistrate upon issuance, “the task of determining what items fell  
7 within broad categories stated in the warrant” and where there were no clear guidelines  
8 distinguishing between property which was subject to search and that which was not. *United*  
9 *States v. Hillyard*, 677 F.2d 1336, 1339 (9th Cir. 1982) (citing *United States v. Drebin*, 557 F.2d  
10 1316, 1322–23 (9th Cir. 1977)); *see also United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995)  
11 (warrant listing fourteen categories of business records without limiting descriptions such as  
12 names of companies involved in illegal scheme was not sufficiently particular); *United States v.*  
13 *Stubbs*, 873 F.2d 210, 211 (9th Cir. 1989) (lack of probable cause to seize all office documents  
14 without reason to believe tax evasion permeated defendant’s entire business).

15 For example, in *Burrows v. Superior Court*, investigators obtained a warrant to search the  
16 office of an attorney accused of misappropriating a client’s funds for “all books, records,  
17 accounts and bank statements and cancelled checks of the receipt and disbursement of money  
18 and any file or documents referring to [four named individuals].” 13 Cal. 3d 238, 241, 248  
19 (1974) (quotation marks omitted). The California Supreme Court held the search unreasonable  
20 because the warrant’s description of the things to be seized was so broad as to authorize a  
21 general search and seizure of the attorney’s financial records without limiting the seizure to  
22 documents regarding the specific persons allegedly involved in the crime. *Id.* at 250 (objecting to  
23 the phrase “any file or documents”).

24 Similarly, in *Aday v. Superior Court*, the court invalidated a warrant to search for  
25 nineteen general categories of documents such as checks, sales records and records connected  
26 with the petitioner’s business. 55 Cal.2d 789, 796 (1961). The court unanimously held the  
27 warrant was fatally overbroad:

1 Articles of the type listed in general terms in the warrant are ordinarily innocuous  
2 and are not necessarily connected with a crime. The various categories, when  
3 taken together, were so sweeping as to include virtually all personal business  
4 property on the premises and placed no meaningful restriction on the things to be  
5 seized. Such a warrant is similar to the general warrant permitting unlimited  
6 search, which has long been condemned.

7 *Id.* These principles should be even more strictly adhered to when officers are conducting  
8 searches of digital information.

9 **B. Overbreadth And Particularity Are Especially Important When Officers**  
10 **Seek Access to Digital Information.**

11 In the age before computers, the particularity requirement was relatively easily  
12 understood as applied during searches of physical spaces. For example, a valid warrant to search  
13 for a rifle in someone's home does not allow officers to open a medicine cabinet where a rifle  
14 could not fit. *See, e.g., Horton v. California*, 496 U.S. 128, 141 (1990).

15 Today, those physical distinctions are no longer a guide. Computer hard drives and online  
16 services contain huge amounts of personal information, both irrelevant material and, potentially,  
17 evidence of criminal behavior. Computers typically contain much information outside the scope  
18 of any particular criminal investigation. As a result, the digital age requires courts to take even  
19 greater care when balancing law enforcement interests with privacy, otherwise digital searches  
20 could "become a vehicle for the government to gain access to data which it has no probable  
21 cause to collect." *United States v. Comprehensive Drug Testing, Inc. (CDT)*, 621 F.3d 1162,  
22 1177 (9th Cir. 2010) (per curiam). The need to search large quantities of electronic records  
23 "creates a serious risk that every warrant for electronic information will become, in effect, a  
24 general warrant, rendering the Fourth Amendment irrelevant." *Id.* at 1176.

25 How should courts deal with these dueling values: law enforcement's legitimate need to  
26 search for evidence of a crime on one hand, and the countervailing prohibition against general  
27 warrants and their evils on the other? While the answer in any given case will of course be fact-  
28 specific, the Fourth Amendment's originating principles are more important than ever as guides.

As technology lowers the barriers to extreme privacy invasions and investigatory  
overreach, the Fourth Amendment must play a critical role in ensuring that the longstanding  
balance between the power and authority of the state and the privacy and liberty of the individual  
[PROPOSED] BRIEF OF AMICI CURIAE ACLU, ACLU OF SOUTHERN CALIFORNIA, AND ACLU OF  
NORTHERN CALIFORNIA IN SUPPORT OF MOTION TO QUASH SEARCH WARRANT  
CASE No. 20CCPC0020

1 does not, either suddenly or through creep, fall constitutionally out of whack. The Fourth  
2 Amendment’s bedrock principles are especially necessary where these technological innovations  
3 facilitate “a too permeating police surveillance.” *Carpenter*, 138 S. Ct. at 2214; *see also Berger*,  
4 388 U.S. at 56 (“The need for particularity . . . is especially great in the case of eavesdropping”  
5 because such surveillance “involves an intrusion on privacy that is broad in scope.”). In some  
6 cases, technology has also given law enforcement the ability to obtain previously unobtainable  
7 information. *Carpenter*, 138 S. Ct. at 2217–18. In cases involving law enforcement’s use or  
8 exploitation of emerging technologies, the Fourth Amendment analysis asks whether the police  
9 conduct threatens to disrupt the traditional “relationship between citizen and government in a  
10 way that is inimical to democratic society.” *United States v. Jones*, 565 U.S. 400, 416 (2012)  
11 (Sotomayor, J., concurring) (quotation marks omitted). This analysis “is informed by historical  
12 understandings ‘of what was deemed an unreasonable search and seizure when [the Fourth  
13 Amendment] was adopted.’” *Carpenter*, 138 S. Ct. at 2214 (alteration in original) (quoting  
14 *Carroll v. United States*, 267 U.S. 132, 149 (1925)); *see also Kyllo v. United States*, 533 U.S. 27,  
15 34 (2001). Courts must ensure that technological innovation does not allow the government to  
16 encroach on the degree of privacy the Fourth Amendment was adopted to protect. *See Carpenter*,  
17 138 S. Ct. at 2214 (cell-site location information); *Kyllo*, 533 U.S. at 34 (thermal imaging).

18 **III. Courts Can Craft Warrants To Constrain Invasive Rummaging—A Risk With**  
19 **Even Seemingly Limited Descriptions of Information.**

20 The point at which an officer seeks a warrant is the best chance a court has to protect  
21 individual privacy interests from unconstitutional invasions. Nothing can truly restore the  
22 confidentiality and integrity of the details of a person’s life once police have combed through  
23 their correspondence and other data. There will very rarely be a case where the probable cause  
24 showing can justify an officer’s request for an “all-content” warrant. Nor are such warrants  
25 necessary as a practical matter; service providers can turn over far more tailored sets of data,  
26 narrowing by type of data, date range, conversation participants, or other variables dictated by  
27 probable cause.

1 That is not to say that anything short of an “all-content” warrant will satisfy the  
2 Constitution. Police seizure of more limited categories of digital information may risk  
3 unconstitutionally overbroad searches and seizures as well. Because electronic storage generally  
4 intermingles responsive and non-responsive data, there is a risk of violating expectations of  
5 privacy in files unrelated to the crime under investigation. In order to ensure that familiar Fourth  
6 Amendment principles remain effective when police conduct such searches, the Ninth Circuit  
7 has recommended that courts implement procedures “to maintain the privacy of materials that  
8 are intermingled with seizable materials, and to avoid turning a limited search for particular  
9 information into a general search of office file systems and computer databases.” *CDT*, 621 F.3d  
10 at 1170. Courts can either impose search conditions at the outset, or can carefully review  
11 investigators’ searches after the fact to ensure that the search was narrowly tailored to probable  
12 cause. If an illegal seizure or search has taken place, the appropriate remedy must include  
13 deletion of all data impermissibly seized. *Id.* at 1177 (the government should return materials  
14 that were not the object of the search once they have been segregated).

15 In sum, courts have tools at hand to manage the dangers of overbroad warrants.

16 **A. Seizures should be limited to relevant categories of information.**

17 There is no need for, and the Fourth Amendment does not allow, “all-content” warrants  
18 demanding seizure of whatever account content or digital files might exist. Rather than issue  
19 “all-content” warrants, courts should only authorize seizure of relevant categories of data. For  
20 example, in one federal investigation of an illegal firearms charge, a search warrant to Facebook  
21 demanded all personal information, activity logs, photos and videos from the user as well as  
22 those posted by others that tag the suspect, all postings, private messages, and chats, all friend  
23 requests, groups and applications activity, all private messages and video call history, check-ins,  
24 IP logs, “likes”, searches, use of Facebook Marketplace, payment information, privacy settings,  
25 blocked users, and tech support requests. *Shipp*, 392 F. Supp. 3d at 303–06. This list was not  
26 limited to the types of information likely to provide evidence of the specific crime under  
27 investigation. The district court expressed “serious concerns regarding the breadth of [the]  
28 Facebook warrants,” pointing out that many of the categories of information were irrelevant to  
[PROPOSED] BRIEF OF AMICI CURIAE ACLU, ACLU OF SOUTHERN CALIFORNIA, AND ACLU OF  
NORTHERN CALIFORNIA IN SUPPORT OF MOTION TO QUASH SEARCH WARRANT  
CASE No. 20CCPC0020

1 probable cause. *Id.* at 307. Moreover, the social media company was in the position to  
2 discriminate between relevant and irrelevant categories of information. The FBI had no need to  
3 seize, for example, Marketplace transaction logs on the grounds that relevant evidence could be  
4 found there. *Id.* at 310.<sup>3</sup>

5 Similarly in *United States v. Wey*, the Southern District of New York held that two  
6 warrants identifying categories of often generic items subject to seizure failed the Fourth  
7 Amendment’s particularity requirement. 256 F. Supp. 3d 355 (S.D.N.Y. 2017). Those categories  
8 included all “financial records, notes, memoranda, records of internal and external  
9 communications, correspondence, audio tapes[] and video tapes, [and] photographs,” among  
10 others. *Id.* at 386 (quotation marks omitted). The only limitation as to the search and seizure was  
11 that the documents had to pertain to the suspects. But because every document seized from the  
12 suspect pertains to the suspect, the court held that the warrants did not impose “meaningful  
13 parameters on an otherwise limitless search of a defendant’s electronic media” and they failed  
14 “to link the evidence sought to the criminal activity supported by probable cause” *Id.* at 387.  
15 Thus, the warrants did “not satisfy the particularity requirement.” *Id.*

16 Courts should authorize seizure of only those categories of data likely to contain evidence  
17 of the crime.

18 **B. Seizures should be limited by time frame and other available characteristics.**

19 Warrants can easily limit data seizures from online providers by time frame. If an offense  
20 allegedly took place in 2019, police may not need to obtain email from any other year, never  
21 mind from the inception of the account, as it did here. *See United States v. Abboud*, 438 F.3d  
22 554, 576 (6th Cir. 2006) (“Failure to limit broad descriptive terms by relevant dates, when such  
23 dates are available to the police, will render a warrant overbroad.” (citations omitted)); *United*  
24 *States v. Diaz*, 841 F.2d 1, 4–5 (1st Cir. 1988) (warrant overbroad when authorized seizure  
25

---

26 <sup>3</sup> Where a social network is the data custodian, concerns that a suspect could effectively disguise  
27 responsive data are relatively minor. *See Shipp*, 392 F. Supp. 3d at 309–10. Still, the *Shipp* court  
28 overstated a suspect’s capacity to effectively hide evidence from officers, given today’s  
sophisticated data analysis tools.

1 records before the first instance of wrongdoing mentioned in the affidavit); *In re*  
2 *[REDACTED]@gmail.com*, 62 F. Supp. 3d 1100, 1104 (N.D. Cal. 2014) (no warrant issued  
3 where government did not include a date limitation); *In re Search of Google Email Accounts*  
4 *identified in Attachment A*, 92 F. Supp. 3d 944 (D. Alaska 2015) (application without date  
5 restriction denied as overbroad).

6 When available, courts can and should also use other criteria of digital information to  
7 constrain police and ensure that seizures are scoped to probable cause. *See United States v.*  
8 *Griffith*, 867 F.3d 1265, 1276 (D.C. Cir. 2017) (deeming a warrant’s failure to narrow a search  
9 based on ownership of a cell phone to be insufficiently particular). For example, if conversations  
10 between Mr. Budnick and either the Los Angeles Probation Department or the Sheriff’s  
11 Department were genuinely potential evidence of a crime, the warrant could demand that Google  
12 turn over only his messages with the relevant government email addresses. *In re Search of Info.*  
13 *Associated With Four Redacted Gmail Accounts*, 371 F. Supp. 3d 843, 845 (D. Or. 2018)  
14 (warrant for all emails associated suspect’s account is overbroad because Google is able to  
15 disclose only those emails the government has probable cause to search). Similarly, Google  
16 Photos is designed to do image searches. *About Google Photos*, Google,  
17 <https://www.google.com/photos/about/> (explaining that photos saved to Google photos “are  
18 organized and searchable by the places and things in them – no tagging required”). Investigators  
19 might seize from Google only those photos that were taken at a particular location or contain a  
20 particular person of interest.

21 **C. Searches Must Be Limited By Probable Cause, And Should Use Clean**  
22 **Teams, Data Deletion, And Other Tools To Protect Privacy.**

23 In some circumstances, investigators will necessarily over-seize electronic data. Even a  
24 well-scoped warrant for social media data or email accounts will include some irrelevant and  
25 innocent information. Often, officers can justify the removal of computers or cell phones from  
26 the scene of a crime—over-seizing the data stored there.<sup>4</sup> Where over-seizure is unavoidable,

27 \_\_\_\_\_  
28 <sup>4</sup> The Ninth Circuit requires the affidavit to explain why practical constraints might require the

1 courts can and should issue warrants that ensure that law enforcement’s subsequent searches of  
2 that data will be cabined to probable cause.

3 The Ninth Circuit in *CDT* suggested limitations courts can impose on search warrants for  
4 intermingled data. *See* 621 F.3d at 1169–71 (opinion of the court); *id.* at 1178–80 (Kozinski,  
5 C.J., concurring) (suggesting limits on retention of unresponsive data, abandonment of the “plain  
6 view” doctrine, and protections for the privacy rights of third parties whose data is intermingled).

7 For example, courts can consider whether to impose a search protocol in the warrant, or  
8 whether to review the search after-the-fact to ensure that it was scoped to probable cause. *See,*  
9 *e.g., In re Search Warrant*, 71 A.3d 1158, 1184 (Vt. 2012); *CDT*, 621 F.3d at 1178–79. The  
10 Ninth Circuit, for example, has expressed a preference for a search protocol, but even in its  
11 absence, “[t]he reasonableness of the officer’s acts both in executing the warrant and in  
12 performing a subsequent search of seized materials *remains subject to judicial review.*” *Hill*, 459  
13 F.3d at 978 (9th Cir. 2006) (emphasis added) (citation omitted).

14 A warrant-issuing court might require the use of independent review teams to “sort[,  
15 segregat[e], decod[e] and otherwise separat[e] seizable data (as defined by the warrant) from all  
16 other data,” so as to shield investigators from exposure to information beyond the scope of the  
17 warrant. *CDT*, 621 F.3d at 1179. Another tool is to require the use of search technology,  
18 including “hashing tools,” to identify responsive files “without actually opening the files  
19 themselves.” *Id.* at 1179 (Kozinski, C.J., concurring).

20 Yet another option is to require police to “waive reliance upon the plain view doctrine in  
21 digital evidence cases,” full stop. In other words, the government must agree not to take  
22 advantage of its own unwillingness or inability to conduct digital searches in a particularized  
23 manner. *Id.* at 1180. Regardless of the method chosen, however, the searches “must be designed  
24 to uncover only the information for which it has probable cause, and only that information may  
25 be examined by the case agents.” *Id.* at 1180 (Kozinski, C.J., concurring).

---

26 seizure of the entire computer system for off-site examination. *See Hill*, 459 F.3d at 975–76  
27 (stating that the affidavit must “demonstrate to the magistrate factually why such a broad search  
28 and seizure authority is reasonable in the case at hand”).

1 Contrary to some government claims, officers need not perform a file-by-file review of  
2 the data on a suspect's computer in every case. Some prosecutors have argued and some courts  
3 have held that because criminals can hide or mislabel files, expansive searches of digital  
4 information are both practically necessary and permissible under the Fourth Amendment. *See,*  
5 *e.g., United States v. Stabile*, 633 F.3d 219, 237 (3d Cir. 2011); *see also United States v.*  
6 *Williams*, 592 F.3d 511, 521 (4th Cir. 2010). But these decisions are premised on an outmoded  
7 understanding of today's technology. Indeed, review of every file in suspects' online accounts or  
8 on their hard drives will often be counterproductive, for it is impractical for an investigator to  
9 manually review the hundreds of thousands of images, files, and messages stored there.

10 An acquired hard drive may contain hundreds of thousands of data files;  
11 identifying the data files that contain information of interest, including  
12 information concealed through file compression and access control, can be a  
13 daunting task. In addition, data files of interest may contain extraneous  
14 information that should be filtered. For example, yesterday's firewall log might  
15 hold millions of records, but only five of the records might be related to the event  
16 of interest.

17 *See Karen Kent et al., Guide to Integrating Forensic Techniques Into Incident Response:*  
18 *Recommendations of the National Institute of Standards and Technology*, No. 800-86 at § 3.2,  
19 U.S. Dep't of Commerce (Aug. 2006), <https://perma.cc/Y2N7-K65R>.

20 Instead, modern forensics tools, widely available today for both criminal investigations  
21 and e-discovery, can search data for file type, dates, and keywords, all without revealing the  
22 contents of non-responsive documents to a human reviewer.

23 Fortunately, various tools and techniques can be used to reduce the amount of  
24 data that has to be sifted through. Text and pattern searches can be used to  
25 identify pertinent data, such as finding documents that mention a particular  
26 subject or person, or identifying e-mail log entries for a particular e-mail address.  
27 Another helpful technique is to use a tool that can determine the type of contents  
28 of each data file, such as text, graphics, music, or a compressed file archive.  
Knowledge of data file types can be used to identify files that merit further study,  
as well as to exclude files that are of no interest to the examination. There are also  
databases containing information about known files, which can also be used to  
include or exclude files from further consideration.

29 *Id.* Some tools can search for categories of images based on the machine's guesses about what a  
30 photo contains. For example, the Blacklight tool can categorize both still images and videos.

1 Their categories are: Alcohol, Child Sexual Abuse Material (CSAM), Currency, Drugs,  
2 Extremism, Gambling, Gore, Porn, Swim/Underwear, and Weapons.<sup>5</sup>

3 In some cases, when a suspect is using sophisticated techniques to hide data, it may make  
4 sense to give officers increased leeway in their search to find potentially hidden information. But  
5 in such a scenario, there should be a probable cause showing of the actor’s “sophisticated”  
6 nature—perhaps, for example, the suspect is a skilled computer programmer who knows how to  
7 manipulate data. But since the scope of a warrant must be limited by probable cause, if a suspect  
8 is not sophisticated, there may be no reason to believe that relevant evidence will be found in  
9 otherwise innocent-seeming places. And even if such concerns apply to search of a suspect’s  
10 own electronic device, they are unlikely to apply to a search of data stored by Google or  
11 Facebook, which structure data storage in ways that make sophisticated concealment difficult.  
12 *See Shipp*, 392 F. Supp. 3d at 308 (discussing the vast and complex nature of Facebook data).

13 Finally, even when a search is reasonable, the government should be required to delete  
14 materials that were not the object of the search once they have been segregated. *See CDT*, 621  
15 F.3d at 1177 (discussing need to segregate nonresponsive information). Expungement is essential  
16 in cases such as this one where the officer’s search and seizure were unconstitutionally  
17 overbroad. *See, e.g., Fazaga v. FBI*, 916 F.3d 1202, 1239 (9th Cir. 2019) (“We have repeatedly  
18 and consistently recognized that federal courts can order expungement of records, criminal and  
19 otherwise, to vindicate constitutional rights.”); *Maurer v. Pitchess*, 691 F.2d 434, 437 (9th Cir.  
20 1982) (“It is well settled that the federal courts have inherent equitable power to order ‘the  
21 expungement of local arrest records as an appropriate remedy in the wake of police action in  
22 violation of constitutional rights.’” (citation omitted)).

23 Courts now are implementing versions of these solutions. For example, in Vermont,  
24 magistrates may design and supervise “targeted searches” by “restricting law enforcement’s  
25 search to those items that met certain parameters based on dates, types of files, or the author of a

---

26 <sup>5</sup> *BlackBag Announces Release of BlackLight 2019 R2*, BlackBag (Sept. 5, 2019),  
27 [https://www.blackbagtech.com/press-releases/blackbag-announces-release-of-blacklight-2019-  
28 r2](https://www.blackbagtech.com/press-releases/blackbag-announces-release-of-blacklight-2019-r2).

1 document.” *See In re Search Warrant*, 71 A.3d at 1184; *see also In re*  
2 *[REDACTED]@gmail.com*, 62 F. Supp. 3d at 1104 (denying a search warrant for a particular  
3 email account because “there is no date restriction of any kind”).

4 And a recent district court case from Michigan helpfully illustrates how courts are now  
5 confronting these issues. In *United States v. Stetkiw*, the government insisted, and the court was  
6 concerned, that, “individuals might hide information in a way that forces a protocol-bound  
7 investigator to overlook it.” No. 18-20579, 2019 WL 2866516, at \*5 (E.D. Mich. July 3, 2019).  
8 Nevertheless, the court held that “an *ex ante* ‘minimization’ requirement can address concerns  
9 about potential Fourth Amendment violations of protocol-less searches, with a goal of decreasing  
10 the amount of non-responsive [electronically stored information] encountered in a search.” *Id.*  
11 (citing Emily Berman, *Digital Searches, the Fourth Amendment, and the Magistrates’ Revolt*, 68  
12 *Emory L.J.* 49, 55 (2018)). The court concluded that *ex ante* procedures would have several  
13 advantages:

14 First, it can minimize the need for *ex post* review of those procedures, which is  
15 often contentious as parties debate motions to suppress evidence in criminal cases. Second, it allows a magistrate judge to closely work with the Government to  
16 ensure its preferred procedures do not violate the Fourth Amendment. Third, it  
17 can promote the development of case law that can distinguish permissible and  
18 impermissible procedures to better protect Fourth Amendment rights. Finally, it  
could prevent situations where certain file locations are authorized for search by  
warrant, but the practical implications of that authorization create a general  
warrant without the magistrate judge’s knowledge.

19 *Id.* While the *Stetkiw* court did not maintain that *ex ante* protocols must be required in every  
20 case, it did suggest that in order to escape such protocols, the government “should demonstrate  
21 that the level of probable cause to search [electronically stored information] is high enough to  
22 justify a search without minimization.” *Id.*

23 Fourth Amendment–compliant searches and seizures not only protect privacy, but serve  
24 law enforcement interests by focusing searches on their proper objects and relevant evidence.  
25 Indeed, one of the biggest problems that officers encounter in investigations involving electronic  
26 data is that they have too much data to make sense of. At the same time, particularity and  
27 overbreadth limitations may be an inconvenience for law enforcement. That is, in part, the point.

28 As one federal judge put it, “[i]t is almost always possible to characterize the Fourth Amendment  
[PROPOSED] BRIEF OF AMICI CURIAE ACLU, ACLU OF SOUTHERN CALIFORNIA, AND ACLU OF  
NORTHERN CALIFORNIA IN SUPPORT OF MOTION TO QUASH SEARCH WARRANT  
CASE No. 20CCPC0020

1 as an inconvenience to law enforcement officials as they carry out their vital duties,” but “[t]hat  
2 inconvenience . . . is one of the fundamental protections that separates the United States of  
3 America from totalitarian regimes.” *Doe v. Prosecutor*, 566 F. Supp. 2d 862, 887 (S.D. Ind.  
4 2008). *See also Johnson v. United States*, 333 U.S. 10, 15 (1948); *United States v. Morgan*, 743  
5 F.2d 1158, 1163–64 (6th Cir. 1984); *United States v. Diggs*, 544 F.2d 116, 130 (3d Cir. 1976).

6 **IV. The Warrant for Mr. Budnick’s Google Account Violates CalECPA, and**  
7 **Everything Provided In Response Should Be Destroyed.**

8 Under California law, Officer Biddle’s warrant in this case was illegally overbroad and  
9 all materials obtained pursuant to the warrant must be destroyed.

10 **A. CalECPA Provides Strong, Clear Digital Privacy Rules For Government,**  
11 **Companies, And The Public.**

12 California has a long tradition of providing more robust privacy protections than federal  
13 law. CalECPA continues that tradition. Passed in 2015, CalECPA establishes clear rules to  
14 protect Californians’ privacy rights when a government entity seeks electronic communications  
15 and device information.

16 *First*, CalECPA requires a probable-cause warrant for all electronic information and  
17 device information, including information sought from third-party service providers or from  
18 personal electronic devices. Cal. Penal Code § 1546.1(a)(2), (a)(3). Under CalECPA, law  
19 enforcement and other California government entities must obtain a warrant to demand people’s  
20 electronic information. This includes everything from emails, digital documents, and text  
21 messages to location and medical information.<sup>6</sup>

22 *Second*, CalECPA specifies the degree of detail that a warrant must contain. Warrants  
23 must “describe with particularity the information to be seized by specifying, as appropriate and  
24 reasonable, the time periods covered, the target individuals or accounts, the applications or

---

25 <sup>6</sup> People also have strong privacy interests in the metadata—which is fully protected by  
26 CalECPA—associated with their accounts, devices, and information. *See generally Metadata:*  
27 *Piecing Together a Privacy Solution*, ACLU of N. Cal. (2014), available at  
28 <https://www.aclunc.org/sites/default/files/Metadata%20report%20FINAL%202021%2014%20cover%202B%20inside%20for%20web%20%283%29.pdf>.

1 services covered, and the types of information sought.” Cal. Penal Code § 1546.1(d)(1).  
2 CalECPA includes heightened particularity requirements specifically because online services and  
3 devices house vast amounts of personal information. As a result, a warrant that permits the  
4 search of a device or online service threatens to intrude upon the privacy not just of the user of  
5 the online service or the holder of the device, but also upon countless others. CalECPA  
6 recognizes that, to effectively protect people’s electronic privacy, the *warrant itself* must restrain  
7 the reach of the government’s power to intrude into our most private digital spaces.

8 *Third*, CalECPA requires that the government entity must provide notice to the target of  
9 any warrant that is contemporaneous with the execution of the warrant. *Id.* § 1546.2(a)(1). While  
10 it is possible for the government to delay that notice, the factual showing required to do so is  
11 extraordinary, limited to circumstances where sworn testimony demonstrates a risk of  
12 endangering life, enabling flight from prosecution, or tampering with evidence or witnesses. *Id.*  
13 § 1546.2(a)(2); *Id.* § 1546.2(b)(2) (defining “adverse result”). And delays, when granted, are  
14 limited to 90 days, with court approval necessary for each extension. *Id.* § 1546.2(b)(2).

15 *Finally*, a core provision of CalECPA is its clear and robust remedies, including both  
16 suppression of evidence and destruction of material obtained in violation of the law. The  
17 suppression remedy is available whenever CalECPA’s rules are violated. Cal. Penal Code  
18 § 1546.4(a). But even before a suppression motion can be filed, CalECPA provides that affected  
19 individuals may petition the court to void the warrant and order destruction of “any information  
20 obtained in violation of [CalECPA], or the California Constitution, or the United States  
21 Constitution.” *Id.* § 1546.4(c).

22 **B. The Search Warrant Failed to Comply with CalECPA.**

23 The search warrant in this case violated CalECPA’s bright-line rules governing the  
24 particularity with which information subject to seizure must be specified and appears to violate  
25 the mandatory provision for notice to targeted individuals.  
26  
27  
28

1                   **1. The Warrant to Mr. Budnick Violates CalECPA’s Particularity**  
2                   **Requirement.**

3                   The warrant in this case seeks “[a]ll records associated with” Mr. Budnick’s Google  
4 Account. Search Warrant for Scott Budnick’s Google Account, Pet. Ex. A, at BS000002. The  
5 warrant then lists, at extraordinary length, examples of information associated captured by that  
6 phrase. The provided list includes essentially every piece of private, sensitive, intimate, or  
7 personal information fathomable: every username, all account activity, every password, every  
8 text message, every email, every physical location (no matter the source), every calendar entry,  
9 every personal contact, every document, every piece of financial information, every photograph,  
10 every mobile app, every search, every call, and every purchase. This is exactly the “virtual  
11 current biography” that the California Constitution protects, and that motivated the authors of  
12 CalECPA to put strong protection for electronic information into the law.<sup>7</sup>

13                   The statute is explicit that warrants shall describe with particularity, “as appropriate and  
14 reasonable, the time periods covered . . . , the applications or services covered, and the types of  
15 information sought.” Cal Penal Code § 1546.1(d)(1). The overbroad warrant in this case, by  
16 sweeping in every piece of information from the target account, without limitation, is the reason  
17 CalECPA exists; there can be no clearer violation of the statute’s command that warrants to  
18 service providers be narrowly tailored and particular.

19                   Even the list of examples, if it were read to be limiting, violates CalECPA. The warrant’s  
20 command that Google produce every piece of information from “[i]nception of account to the

21 <sup>7</sup> See *People v. Chapman*, 36 Cal.3d 98, 108–109 (1984); Bill Analysis, Assembly Committee on  
22 Privacy and Consumer Protection 9–10, SB 178 (June 23, 2015) (“SB 178 updates existing  
23 federal and California statutory law for the digital age and codifies federal and state  
24 constitutional rights to privacy and free speech by instituting a clear, uniform warrant rule for  
25 California law enforcement access to electronic information, including data from personal  
26 electronic devices, emails, digital documents, text messages, metadata, and location information.  
27 Each of these categories can reveal sensitive information about a Californian’s personal life: her  
28 friends and associates, her physical and mental health, her religious and political beliefs, and  
more. The California Supreme Court has long held that this type of information constitutes a  
‘virtual current biography’ that merits constitutional protection. SB 178 would codify that  
protection into statute. SB 178 also ensures that proper notice, reporting, and enforcement  
provisions are also updated and in place for government access to electronic information and to  
ensure that the law is followed.”).

1 date this warrant is signed” fails to include reasonable particularity with respect to the time  
2 periods covered, as the statute mandates. Def. Ex. A, at BS000002; *see also* Cal Penal Code  
3 § 1546.1(d)(1). And in requesting “[a]ll applications downloaded, installed, and/or purchased by  
4 the associated account and/or device” the warrant additionally fails to specify the “applications  
5 or services covered,” opting instead to seize every application. Def. Ex. A, at BS000003; Cal  
6 Penal Code § 1546.1(d)(1).

7 CalECPA was written with the threat of unlimited warrants like the one in this case in  
8 mind. As the author wrote, “Law enforcement is increasingly taking advantage of outdated  
9 privacy laws to turn mobile phones into tracking devices and to access emails, digital documents,  
10 and text messages without proper judicial oversight.”<sup>8</sup> Importantly, CalECPA protects not just  
11 people, but the companies who operate services for consumers in California. Those companies,  
12 as the author highlighted, “are increasingly concerned about the loss of consumer trust and its  
13 business impact, and are in need of a consistent statewide standard for law enforcement  
14 requests.”<sup>9</sup> If warrants like the one in this case are allowed, consumer trust in both service  
15 providers and government will be further undermined.

16 For these reasons, CalECPA puts in place statutory mandates limiting law enforcement  
17 access to exactly the sources of information at issue here, and it demands strict judicial oversight  
18 when those mandates are not followed.

## 19 **2. Mr. Budnick May Not Have Received Notice Required by CalECPA.**

20 CalECPA also inaugurated a powerful and detailed notice regime commanding law  
21 enforcement to inform targets of investigations when warrants are executed. The notice  
22 requirements under CalECPA go far beyond mere clerical or procedural requirements and create  
23 new and important rights for individuals whose information is captured by law enforcement  
24 pursuant to a warrant.

---

26 <sup>8</sup> Bill Analysis, Assembly Committee on Public Safety 12, SB 178 (July 14, 2015).

27 <sup>9</sup> *Id.* at 13.

1 As the legislature recognized explicitly, CalECPA’s notice requirements go beyond  
2 federal law, under which “a governmental entity is not required to provide notice to a subscriber  
3 or customer when a warrant is obtained for specified electronic information.” Bill Analysis,  
4 Privacy: Electronic Communications: Search Warrants 7, Senate Committee on Appropriations,  
5 SB 178 (April 22, 2015). These new individualized notice rights were a central focus of the  
6 legislature because of their significant fiscal impact. *Id.* Both the requirement that the target  
7 individual be notified in ordinary circumstances when the warrant is executed, *and* the  
8 requirement that even more detailed notice be provided when the original notice is delayed, were  
9 carefully considered by the legislature and determined to be worth the cost.<sup>10</sup> In sum, CalECPA  
10 created new, strict, and powerful notice rights for the targets of warrants in California.

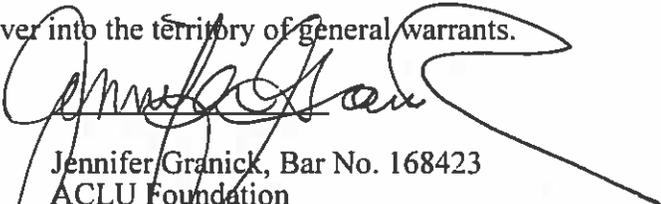
11 All targets of a warrant must, under ordinary circumstances, receive notice  
12 contemporaneously with the execution of the warrant. Cal. Penal Code § 1546.2(a)(7). That  
13 notice can be delayed, but for no longer than 90 days at a time, and each such delay requires  
14 separate court authorization. *Id.* § 1546.2(b)(1). If the government obtains a delay, the statute  
15 requires that the later notice be even more extensive. In addition to notifying the target that the  
16 warrant has been executed, any notice provided after a period of delay must also include “a copy  
17 of all electronic information obtained or a summary of that information, including, *at a*  
18 *minimum*, the number and types of records disclosed, the date and time when the earliest and  
19 latest records were created, and a statement of the grounds for the court’s determination to grant  
20 a delay in notifying the individual.” *Id.* § 1546.2(b)(3) (emphasis added).

21  
22  
23  
24  
25 <sup>10</sup> Bill Analysis, Assembly Committee on Appropriations 1–2, SB 178 (May 28, 2015) (“[U]nder  
26 existing federal law, a governmental entity may require a provider of electronic communication  
27 service to disclose a record or other information pertaining to a subscriber to or customer of such  
28 service under specified circumstances, including pursuant to a warrant or court order. A  
governmental entity receiving records or information under this provision of federal law is not  
required to provide notice to a subscriber or customer.” (citing 18 USC § 2703)).



1 could take advantage of the tools at their disposal to ensure that these types of investigations are  
2 particular and narrow, and do not cross over into the territory of general warrants.

3 Dated: February 24, 2020



Jennifer Granick, Bar No. 168423  
ACLU Foundation  
39 Drumm Street  
San Francisco, CA 94111  
415-343-0758  
jgranick@aclu.org

Jacob A. Snow, Bar No. 270988  
ACLU Foundation of Northern California  
39 Drumm Street  
San Francisco, CA 94111  
415-621-2493  
jsnow@aclunc.org

Peter Bibring, Bar No. 223981  
Mohammad Tajsar, Bar No. 280152  
ACLU Foundation of Southern California  
1313 West 8<sup>th</sup> Street  
Los Angeles, CA 90017  
213-977-5295  
pbibring@aclusocal.org  
mtajsar@aclusocal.org

*On the brief:*  
Brett Max Kaufman  
Alexia Ramirez  
Nathan Freed Wessler  
ACLU Foundation  
125 Broad Street, 18th Floor  
New York, NY 10004  
212-549-2500  
bkaufman@aclu.org  
aramirez@aclu.org  
nwessler@aclu.org

**AUG 31 2020**

Sherri R. Carter, Executive Officer/Clerk of Court  
By Sheryl R. Humber Deputy  
Sheryl R. Humber

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**SUPERIOR COURT OF THE STATE OF CALIFORNIA  
FOR THE COUNTY OF LOS ANGELES  
CLARA SHORTRIDGE FOLTZ CRIMINAL JUSTICE CENTER  
CRIMINAL WRITS CENTER**

In re ) **Case No.: BH012910**  
SEARCH WARRANT TO GOOGLE FOR )  
ALL RECORDS ASSOCIATED WITH ) **ORDER RE: MOTION TO QUASH SEARCH**  
GOOGLE ACCOUNT ) **WARRANT**  
SCOTTARCLA@GMAIL.COM )

**AFTER A HEARING**

Motion to quash search warrant, return property, and destroy all seized information, filed by Petitioner Scott Budnick, represented by Alan J. Jackson, Esq.; Kelly C. Quinn, Esq.; and Mehrunisa Ranjha, Esq. Respondents, the County of Los Angeles and the Los Angeles County Sheriff's Department (LASD), represented by Raymond J. Fuentes, Esq., and John L. Fuentes, Esq. **Granted.**

**BACKGROUND**

Petitioner is a civilian who spends a significant amount of his time working as a juvenile justice advocate, which includes lobbying for legislative reform, advocating for educational programs in the juvenile justice system, and assisting minors charged with crimes. Petitioner is not an attorney. Petitioner became involved in the case of Abel Diaz, who was charged with the

1 murder of a police officer.<sup>1</sup> Through the Diaz case, Petitioner caught the attention of Sergeant  
2 Richard Biddle, who had been investigating the case and had authored several prior warrants  
3 related to the case.

4 On April 3, 2019, Judge Michael E. Pastor, acting as magistrate, signed a search warrant  
5 for all records associated with the Google account scottarcla@gmail.com, which belongs to  
6 Petitioner, from the date of inception, including all emails, financial records, location data,  
7 search history, call records, voice messages, and multimedia messages. An order to delay  
8 notification of the search warrant for 90 days was also signed on the same date.

9 The warrant incorporated several previously obtained search warrants by reference,  
10 including a warrant obtained for the search of the scottarc@gmail.com Google account. (Search  
11 Warrant (Warrant), dated Apr. 3, 2019, attached to mtn. as exh. A, at p. 10.) The warrant was  
12 obtained as part of an investigation into alleged criminal activities including conspiracy to  
13 obstruct justice (Pen. Code, § 182, subd. (a)(5)),<sup>2</sup> conspiring to offer false evidence in judicial  
14 proceedings (§ 132), conspiring to destroy/conceal evidence (§ 135), conspiring to intimidate  
15 witnesses (§ 136), conspiring to induce false testimony (§ 137), conspiring to violate court orders  
16 (§ 166.4), conspiring to illegally communicate or contact a prisoner (§ 4570), and conspiring to  
17 tamper with records or documents in possession of a government agency (Gov. Code, § 6200).  
18 (*Ibid.*)

19  
20 On February 19, 2020, Petitioner filed a motion to quash the search warrant, return  
21 property, and destroy all seized information. Petitioner contends that the warrant was not  
22 supported by probable cause, that the warrant was based on prior warrants that were also illegal,  
23 and that the warrant violated the California Electronic Communications Privacy Act (CalECPA),  
24 sections 1546 to 1546.4, in its breadth and scope. On March 16, 2020, the court signed and filed  
25

26  
27 <sup>1</sup> Diaz's case was ultimately adjudicated in the Juvenile Division of this court, where he  
28 was found to be responsible for the death of a police officer.

<sup>2</sup> All further undesignated statutory references are to the Penal Code.

1 a protective order preventing Respondent from accessing, viewing, copying, manipulating,  
2 disseminating, or interacting in any way with the property seized pursuant to the search warrant.  
3 On March 16, 2020, the American Civil Liberties Union and the American Civil Liberties Union  
4 of Northern and Southern California filed a brief in support of the motion to quash as amici  
5 curiae, which the court allowed. On March 25, 2020, Respondent filed an ex parte application  
6 for an order to vacate the protective order. On March 26, 2020, Petitioner filed an opposition to  
7 Respondent's ex parte application. The court declined to sign a proposed order included with the  
8 ex parte application, noting that it was not an ex parte matter. On April 14, 2020, Respondent  
9 filed an opposition to the motion to quash. On July 2, 2020, Petitioner filed a reply to  
10 Respondent's opposition to the motion to quash. On July 7, 2020, the court conducted a hearing  
11 on the motion, and took the matter under submission.  
12

### 13 SUMMARY OF WARRANT<sup>3</sup>

14 As discussed *ante*, the April 3, 2019 warrant that is the subject of the instant motion  
15 sought all records associated with the Google account scottarcla@gmail.com from the date of  
16 inception, including all emails, financial records, location data, search history, call records, voice  
17 messages, and multimedia messages. (Warrant at pp. 2–3.) The justification for the 90-day  
18 delay in notification of the warrant was the belief that notification of the warrant's existence  
19 would cause destruction of or tampering with the evidence to occur. (*Id.* at p. 6.) The warrant  
20 was obtained as part of an ongoing investigation into alleged criminal activities including  
21 conspiracy to obstruct justice (§ 182, subd. (a)(5)), conspiring to offer false evidence in judicial  
22 proceedings (§ 132), conspiring to destroy/conceal evidence (§ 135), conspiring to intimidate  
23 witnesses (§ 136), conspiring to induce false testimony (§ 137), conspiring to violate court orders  
24 (§ 166.4), conspiring to illegally communicate or contact a prisoner (§ 4570), and conspiring to  
25 tamper with records or documents in possession of a government agency (Gov. Code, § 6200).  
26

---

27 <sup>3</sup> The instant warrant consists of hundreds of pages, which both parties are familiar with.  
28 Therefore, the following summary contains only a general description of the contents of the  
warrant and its numerous attachments.

1 (*Id.* at p. 10.) Attached and incorporated in the instant warrant was a previous search warrant,  
2 which itself incorporated another previous warrant, which then incorporated other previous  
3 warrants, and so forth, in a situation not dissimilar to a set of nesting dolls. (Hearing Transcript  
4 (“HT”), dated Jul. 7, 2020, at p. 4.)

5 Sergeant Biddle related his extensive training and experience investigating criminal  
6 activity, specifically regarding assaults, robberies, burglaries, narcotics, gang behavior, fraud,  
7 identity theft, and homicide. (Warrant at p. 8.) Sergeant Biddle stated that he has received  
8 training regarding cellular phones as related to criminal investigations, and is of the opinion that  
9 “regardless of the crime, it is likely the suspect used a cell phone before, during, or after the  
10 commission of the crime.” (*Id.* at pp. 8–9.) Sergeant Biddle asserted that he has become  
11 familiar with social media websites and that people occasionally post incriminating photographs  
12 or writings on social media accounts, which can prove useful in prosecuting criminal cases. (*Id.*  
13 at p. 10.)

14  
15 Sergeant Biddle stated his belief that Petitioner’s Google account would contain  
16 communications between Petitioner and members of the Office of the District Attorney, the  
17 LASD, and the Los Angeles County Probation Department (Probation Department)  
18 “documenting inappropriate and potential criminal acts regarding [Petitioner’s] involvement in  
19 obstructing justice and other criminal conduct . . . .” (Warrant at p. 11.) He also stated his belief  
20 that the account would contain evidence of an “ongoing conspiracy to alter, remove, falsify, or  
21 conceal records and or documents in possession of government agencies” and would identify co-  
22 conspirators of Petitioner’s. (*Ibid.*) Additionally, Sergeant Biddle stated that the account would  
23 contain communications regarding Petitioner “inappropriately providing legal advice to adult and  
24 juvenile criminal defendants.” (*Ibid.*) Sergeant Biddle attached and incorporated a February 27,  
25 2019 search warrant for the scottarc@gmail.com email address, which he apparently mistakenly  
26 believed was Petitioner’s email address. (*Id.* at p. 10.)  
27  
28

1 The attached February 27, 2019 warrant included a transcript of a jail call between  
2 Petitioner and Diaz from July 2015 in which Petitioner discussed Diaz's pending criminal case  
3 and the process for hiring a new lawyer for Diaz, as well as a transcript of a call from December  
4 2015 in which Petitioner again discussed Diaz's pending criminal case. (Warrant at pp. 21–33.)  
5 Sergeant Biddle alleged that these transcripts provided evidence of Petitioner's "involvement in  
6 criminal proceedings and his on-going conspiracies to obstruction of justice." (*Id.* at p. 33.) He  
7 alleged that the calls documented Petitioner stating that he communicated with people in the  
8 District Attorney's Office regarding Diaz's case and showed that Petitioner provided  
9 "inappropriate legal advice" to Diaz without Diaz's attorney's knowledge or permission. (*Ibid.*)

10 Attached to the February 27, 2019 warrant was another warrant, this warrant being for the  
11 search of Probation Department email accounts for any emails about Petitioner, Diaz's attorney  
12 Michael Cavalluzzi, or search warrants. (Warrant at p. 39.) The warrant alleged that the  
13 requested emails contained evidence regarding "conspiracy to obstruct justice, conspiracy to  
14 provide false evidence in judicial proceedings, witness dissuading, conspiracy to facilitate illegal  
15 communications with in custody defendants, and conspiracy to conceal evidence related to a  
16 criminal investigation." (*Ibid.*) A similar warrant was attached regarding LASD emails. (*Id.* at  
17 pp. 42–44.) Attached to these warrants were anonymous letters alleging inappropriate conduct  
18 between Petitioner and the Probation Department; search warrants dated August 2, 2017, and  
19 April 14, 2017, for Probation Department records related to Petitioner's contact with Diaz;  
20 reports regarding Diaz's participation in juvenile programming; reports regarding alleged  
21 violations of Probation Department policies by Petitioner; reports containing allegations of  
22 misconduct and inappropriate physical contact with juveniles by Petitioner; and reports regarding  
23 the Probation Department's failure to comply with search warrants for information regarding  
24 Petitioner. (*Id.* at p. 46.) Additionally, a search warrant for the homes of family members of  
25 Diaz was attached, as well as reports and evidence associated with that search warrant. (*Id.* at p.  
26  
27  
28

1 47.) Lastly, a report regarding the arrest and interview of Jose Alvarado, Diaz's brother, was  
2 attached. (*Ibid.*)

3 Sergeant Biddle alleged in the warrant for emails from the Probation Department that  
4 Petitioner and Diaz's attorneys advocated for Diaz to remain in Juvenile Hall pending transfer to  
5 the Department of Juvenile Justice, after Diaz entered into a plea agreement. (Warrant at p. 48.)  
6 Sergeant Biddle alleged that Diaz would sign into classes at Juvenile Hall and then return to his  
7 dorm without attending the classes. (*Id.* at p. 47.) Sergeant Biddle alleged that Petitioner called  
8 jail inmates and discussed disciplinary proceedings with them, as well as support letters and  
9 recommendation letters authored by Petitioner. (*Id.* at pp. 49–50.) Sergeant Biddle also stated  
10 that Petitioner previously received a reprimand from the LASD for violating jail policies and that  
11 at one point in 2019, Petitioner's volunteer status was revoked by the LASD. (*Id.* at p. 50.)

12 The attached anonymous letter from the Probation Department expressed concern over  
13 possible policy violations perpetrated by Petitioner during his meetings with Diaz and his  
14 discussions with Diaz about the criminal case. (Warrant at p. 55.) An attached Probation  
15 Department special incident report described an incident wherein Petitioner was granted access  
16 to the Probation Department because he "had the Probation Chief on speed dial." (*Id.* at p. 56.)  
17 The report also described Petitioner's cell phone use in the facility. (*Id.* at p. 57.) An attached  
18 2017 LASD complaint report co-authored by Sergeant Biddle discussed various recorded jail  
19 phone calls with Petitioner where he discussed details of pending criminal cases with juveniles,  
20 including in some instances advising them to fire their current attorneys, as well as instances of  
21 Probation Department policy violations. (*Id.* at pp. 59–71.)

22 A 2017 warrant for the search of Probation Department and Juvenile Hall records for any  
23 files or records related to Diaz was attached, including for mental health records and entries in  
24 the Juvenile Hall Log Book for Petitioner and any known associates. (Warrant at pp. 72–94.)  
25 The affidavit attached to the warrant also contained a summary of jail calls between Petitioner  
26 and inmates, including Diaz, where Petitioner discussed details of pending criminal cases. (*Id.* at  
27  
28

1 pp. 81–87.) A subpoena duces tecum for Probation Department records was attached. (*Id.* at pp.  
2 95–105.) Many documents previously mentioned were duplicated as what appear to be  
3 attachments to the 2017 warrant discussed *ante*. Additional jail call summaries were included.  
4 (*Id.* at pp. 123–144, 151–159.) A summary of Diaz’s probation records was also attached,  
5 including mental health records and disciplinary records. (*Id.* at pp. 145–150, 160–165.)

6 A summary of a conversation Sergeant Biddle had with Scott Sanders of the Probation  
7 Department in 2017 was attached, in which Sanders described alleged policy violations by  
8 Petitioner, as well as the process of producing Diaz’s records. (Warrant at pp. 166–171.) A  
9 summary of a 2018 meeting between Sergeant Biddle, two prosecutors, Probation Department  
10 staff, and several other law enforcement officers was attached, in which Petitioner’s relationship  
11 with juveniles was described. (*Id.* at pp. 172–175.) A summary of the search warrant service on  
12 the Probation Department was also included. (*Id.* at pp. 177–178.)

13 A 2018 search warrant for Diaz’s living space at Juvenile Hall; Maricela Alvarado’s  
14 (Diaz’s sister) home, person, and cell phone; Jose Alvarado’s home, person, and cell phone; and  
15 Miguel Garcia’s person and cell phone was included. (Warrant at pp. 182–207.) That warrant  
16 sought evidence of 18 Street Gang criminal activity. (*Ibid.*) A report of an interview with  
17 Garcia regarding his gang activity and relationship with Diaz was included. (*Id.* at pp. 208–212.)  
18 A report of an interview with Adrian Nava, the husband of Maricela Alvarado, regarding his  
19 connection to the 18 Street Gang, threats received by Maricela Alvarado, and his connection to  
20 Diaz and Petitioner was also included. (*Id.* at pp. 213–218.) Additional reports regarding Nava  
21 were also included, which included discussion of Petitioner and Diaz’s attorneys’ activities in  
22 relation to Diaz’s case. (*Id.* at pp. 219–234.)

23 A 2018 report of the results of the search warrant served on Maricela Alvarado was  
24 attached. (Warrant at pp. 235–240.) A 2018 report of the results of the search of Garcia’s and  
25 Maricela Alvarado’s cell phones was also attached, including a description of a photo of  
26 Petitioner with Diaz’s family. (*Id.* at pp. 241–246.) Additionally, a 2018 report of the arrest and  
27  
28

1 interview of Jose Alvarado, including some discussion of things Petitioner did to assist Diaz with  
2 his case, was attached. (*Id.* at pp. 247–252.) Another attached 2018 report included details of  
3 jail calls made by Alvarado, including conversations with Diaz’s attorney; notes about  
4 Petitioner’s meetings with Diaz, allegedly without the consent of Diaz’s attorney; notes about  
5 Diaz’s attorneys’ conduct; and descriptions and transcripts of recorded Juvenile Hall calls. (*Id.*  
6 at pp. 253–321.)

#### 7 APPLICABLE LAW

8 The United States and California constitutions require a finding of probable cause before  
9 a search warrant may be issued. (U.S. Const., 4th Amend.; Cal. Const., art. 1, § 13.) This  
10 requirement is codified in section 1525, which states that “[a] search warrant cannot be issued  
11 but upon probable cause, supported by affidavit, naming or describing the person to be searched  
12 or searched for, and particularly describing the property, thing, or things and the place to be  
13 searched.”  
14 searched.”

15 “[P]robable cause is a flexible, common-sense standard.” (*Texas v. Brown* (1983) 460  
16 U.S. 730, 742.) “A ‘practical, nontechnical’ probability that incriminating evidence is involved  
17 is all that is required.” (*Ibid.*, quoting *Brinegar v. United States* (1949) 338 U.S. 160, 176.)  
18 “This is not to say that probable cause can be made out by affidavits which are purely  
19 conclusory, stating only the affiant’s . . . belief that probable cause exists without detailing any of  
20 the ‘underlying circumstances’ upon which that belief is based.” (*U.S. v. Ventresca* (1965) 380  
21 U.S. 102, 108.)

22 The test for probable cause is based on the totality of the circumstances, which allows  
23 deficiencies in one area to be compensated for by strengths in another, and ultimately tasks the  
24 issuing magistrate with making “a practical, common-sense decision whether, given all the  
25 circumstances set forth in the affidavit before him . . . there is a fair probability that contraband  
26 or evidence of a crime will be found in a particular place.” (*Illinois v. Gates* (1983) 462 U.S.  
27 213, 233, 238.) “Sufficient information must be presented to the magistrate to allow that official  
28

1 to determine probable cause; his action cannot be a mere ratification of the bare conclusions of  
2 others. In order to ensure that such an abdication of the magistrate’s duty does not occur, courts  
3 must continue to conscientiously review the sufficiency of affidavits on which warrants are  
4 issued.” (*Id.* at p. 239.) The totality of the circumstances test has been adopted by California  
5 courts. (*People v. Brueckner* (1990) 223 Cal.App.3d 1500, 1504.)

6 In 2014, the United States Supreme Court held that a search warrant is required to search  
7 the contents of a cell phone, noting that cell phones contain “detailed information about all  
8 aspects of a person’s life.” (*Riley v. California* (2014) 573 U.S. 373, 396, 403 (“*Riley*”).)  
9 CalECPA was enacted in California after the holding in *Riley*. Pursuant to CalECPA, a warrant  
10 seeking access to electronic communication information must “describe with particularity the  
11 information to be seized by specifying, as appropriate and reasonable, the time periods covered,  
12 the target individuals or accounts, the applications or services covered, and the types of  
13 information sought . . . .” (§ 1546.1, subd. (d)(1).)

14 CalECPA also includes a notice requirement. Section 1546.2, subdivision (a)(1), states  
15 that the target of the warrant must be provided notice contemporaneously with execution of the  
16 warrant, stating with reasonable specificity the nature of the investigation. “The notice shall  
17 include a copy of the warrant or a written statement setting forth facts giving rise to the  
18 emergency.” (§ 1546.2, subd. (a)(1).) If the court finds reason to believe that notification may  
19 trigger an adverse result, the court may order delayed notification, not to exceed 90 days. (§  
20 1546.2, subd. (b)(1).) An “adverse result” is defined as either danger to the life or physical  
21 safety of an individual, flight from prosecution, destruction or tampering with evidence,  
22 intimidation of potential witnesses, serious jeopardy to an investigation, or undue delay of a trial.  
23 (§ 1546, subd. (a).)

24 ///

25 ///

26 ///

27 ///

28 ///

1 DISCUSSION

2 Proper Respondent

3 Petitioner briefly argues that there is no respondent in the instant case, and that counsel  
4 for the County of Los Angeles and LASD should not have been permitted to appear on the  
5 motion and defend the warrant. The court acknowledges the unique nature of the instant  
6 proceeding, but allows counsel for the County of Los Angeles and LASD to appear as  
7 Respondent due to the apparent absence of any other suitable respondent in this case. The court  
8 is cognizant, however, that its review of the warrant is limited to the four corners of the  
9 document, and renders its ruling with that principle in mind. (*People v. Frank* (1985) 38 Cal.3d  
10 711, 729.)

11 CalECPA

12 As discussed *ante*, CalECPA details specific requirements for a warrant seeking access to  
13 electronic communication information. These requirements appear to have been completely  
14 disregarded in the instant case. As discussed *ante*, a warrant for electronic communication  
15 information must state with particularity the information to be seized, the time period to be  
16 covered, the applications and services covered, and the information sought. (§ 1546.1, subd.  
17 (d)(1).) The instant warrant made no attempt to limit the amount of information to be searched.  
18 General warrants permitting unlimited searches have “long been condemned,” even before the  
19 advent of smart phones and the passage of CalECPA. (*Aday v. Superior Court* (1961) 55 Cal.2d  
20 789, 796.) In the digital age, particularity and specificity in search warrants are more important  
21 than ever.

22  
23 The warrant sought all information associated with the account from the date of  
24 inception. It is not an overstatement to describe this warrant as seeking access to Petitioner’s  
25 entire electronic existence, which likely contains details about his entire life, including  
26 everywhere he has been, everyone he has communicated with, every financial transaction he has  
27 made, and every piece of information he has searched for since he created the account. As  
28

1 seemingly no attempt was made to limit the scope of the search, it is impossible to conclude that  
2 the warrant complied with the particularity requirements of CalECPA. Even if the warrant was  
3 supported by probable cause, discussed *post*, the court would still be required to invalidate the  
4 warrant as it does not meet the particularity requirements of CalECPA.

5         Petitioner also contends that the warrant did not comply with the notice requirement of  
6 CalECPA. The court notes that the magistrate did find that notification of the existence of the  
7 warrant would have had an adverse result, and signed an order to delay notification of the search  
8 warrant as required by section 1546.2, subdivision (b)(1). On its face, the warrant appears to  
9 have complied with CalECPA's notice requirement. Nevertheless, as discussed *ante*, the warrant  
10 failed to meet the requirements of section 1546.1, subdivision (d)(1).

#### 11 Probable Cause

12         The instant warrant, although lengthy, failed to establish probable cause. The court notes  
13 that broad generalizations, even when based on law enforcement experience regarding the habits  
14 of criminals, do not establish probable cause. (*People v. Pressey* (2002) 102 Cal.App.4th 1178,  
15 1185.) A finding of probable cause cannot be made from an affidavit that is purely conclusory.  
16 (*U.S. v. Ventresca, supra*, 380 U.S. at p. 108.) An affidavit must contain detailed circumstances  
17 with reasons why the source of the information is credible. (*Id.* at pp. 108–109.)

18         When the gloss of advocacy is stripped away, the instant warrant simply did not establish  
19 probable cause for the overwhelmingly invasive search requested. The warrant was painfully  
20 short on actual facts, instead composed of conclusory allegations and speculation by Sergeant  
21 Biddle. The warrant was extremely lengthy and difficult to navigate, consisting of multiple  
22 interconnected and self-referential documents, including several previous search warrants. Much  
23 of the information contained was duplicative. No facts were presented supporting allegations of  
24 actual illegal conduct by Petitioner, much less the broad conspiracies penetrating multiple  
25 government agencies alleged in the instant warrant. While certain conduct was alleged to be  
26 inappropriate, or to constitute a policy violation, neither inappropriate conduct nor policy  
27  
28

1 violations provide probable cause for an overbroad and intrusive search warrant such as the one  
2 in the instant case.

3 Conduct such as providing legal advice to Diaz or contacting officials in the District  
4 Attorney's Office or the Probation Department regarding the case does not constitute a crime.  
5 Petitioner is not an attorney and is not bound by the ethical rules governing the profession, but  
6 even if he was, the actions described in the instant warrant would hardly constitute criminal  
7 activity. The warrant quite simply did not contain allegations of criminal activity supported by  
8 any concrete facts. The warrant certainly did not contain allegations sufficient to justify access  
9 to Petitioner's entire electronic existence.

10 The court finds that, considering the totality of the circumstances, the warrant challenged  
11 in the instant motion was not supported by probable cause. As the court finds that the instant  
12 warrant was not supported by probable cause, the court does not reach Petitioner's arguments  
13 regarding the legality of the previous warrants referenced in the instant warrant and any allegedly  
14 tainted evidence obtained pursuant to those warrants.

15  
16 Remedy

17 Respondent suggests in the opposition to the motion to quash that if the court were to find  
18 portions of the warrant invalid, the court should then invalidate and sever those portions of the  
19 warrant without invalidating the warrant in its entirety. Petitioner alleges that this is not an  
20 appropriate remedy pursuant to CalECPA, and argues that the only appropriate remedy is to  
21 completely quash the warrant.

22 Section 1546.4, subdivision (a), states that any person "may move to suppress any  
23 electronic information obtained or retained in violation of the Fourth Amendment to the United  
24 States Constitution or of [CalECPA]." Section 1546.4, subdivision (c), states that an individual  
25 targeted by a warrant "may petition the issuing court to void or modify the warrant . . . ." While  
26 it appears that the court does have the discretion to modify the warrant pursuant to section  
27  
28

1 1546.4, subdivision (c), the court agrees with Petitioner that the proper remedy in this case is to  
2 quash the search warrant, return all seized property, and destroy all seized information.

3 As discussed *ante*, the warrant was lacking in probable cause and failed to comply with  
4 any of CalECPA's particularity requirements. It does not appear to the court that some portions  
5 of the warrant may be valid, when the warrant as a whole was in violation of CalECPA. As  
6 Respondent made no attempt to sufficiently tailor the warrant initially, the court will not now  
7 attempt to undertake the onerous task of sifting through the voluminous documents in order to  
8 recover salvageable portions of the warrant, assuming for the sake of argument that any exist.

9  
10 DISPOSITION

11 For all of the foregoing reasons, the motion to quash the April 3, 2019 search warrant,  
12 return property, and destroy all seized information is GRANTED. The Los Angeles County  
13 Sheriff's Department is ORDERED TO RETURN within 10 calendar days of the service of this  
14 order all property seized pursuant to the warrant and destroy all information in its possession  
15 obtained pursuant to the warrant. Within 30 days of service of this order the Los Angeles County  
16 Sheriff's Department is to file and serve a return with this court, under penalty of perjury, as  
17 evidence that it has fully complied with this order.

18 The Clerk is ordered to serve a copy of this order upon Alan J. Jackson, Esq.; Kelly C.  
19 Quinn, Esq.; and Mehrunisa Ranjha, Esq., as counsel for Petitioner, and upon Raymond J.  
20 Fuentes, Esq., and John L. Fuentes, Esq., as counsel for Respondents, the County of Los Angeles  
21 and the Los Angeles County Sheriff's Department.

22  
23  
24 Dated: 8-31-20



25   
26 WILLIAM C. RYAN  
27 Judge of the Superior Court  
28

1 **Send a copy of this order to:**

2 Alan J. Jackson, Esq.  
3 Kelly C. Quinn, Esq.  
4 Mehrunisa Ranjha, Esq.  
5 WERKSMAN JACKSON & QUINN LLP  
6 888 West Sixth Street, Fourth Floor  
7 Los Angeles, CA 90017

8 Raymond J. Fuentes, Esq.  
9 John L. Fuentes, Esq.  
10 Fuentes & McNally, LLP  
11 700 North Central Avenue, Suite 450  
12 Glendale, CA 91203-2602

13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

<b>SUPERIOR COURT OF CALIFORNIA COUNTY OF LOS ANGELES</b>	Reserved for Clerk's File Stamp
COURTHOUSE ADDRESS: Clara Shortridge Foltz Criminal Justice Center 210 West Temple Street Los Angeles, CA 90012	<b>FILED</b> Superior Court of California County of Los Angeles
PLAINTIFF/PETITIONER  In re: SEARCH WARRANT TO GOOGLE FOR ALL RECORDS ASSOCIATED WITH GOOGLE ACCOUNT SCOTTARCLA@GMAIL.COM	<b>AUG 31 2020</b>  Sherri R. Carter, Executive Officer/Clerk of Court By <u><i>Sherri R. Carter</i></u> Deputy Sheryl R. Humber
<b>CLERK'S CERTIFICATE OF MAILING</b> CCP, § 1013(a) Cal. Rules of Court, rule 2(a)(1)	CASE NUMBER: <b>BH012910</b>

I, the below-named Executive Officer/Clerk of the above-entitled court, do hereby certify that I am not a party to the cause herein, and that this date I served:

- |  |   |
|--|---|
| <input type="checkbox"/> Order Extending Time            | <input checked="" type="checkbox"/> Order re: Motion to Quash Search Warrant  |
| <input type="checkbox"/> Order to Show Cause             | <input type="checkbox"/> Order re: Eligibility  |
| <input type="checkbox"/> Order for Informal Response     | <input type="checkbox"/> Order re: Appointment of Counsel   |
| <input type="checkbox"/> Order for Supplemental Pleading | <input type="checkbox"/> Copy of Petition for Writ of Habeas Corpus /Suitability<br>Hearing Transcript for the Attorney General |

I certify that the following is true and correct: I am the clerk of the above-named court and not a party to the cause. I served this document by placing true copies in envelopes addressed as shown below and then by sealing and placing them for collection; stamping or metering with first-class, prepaid postage; and mailing on the date stated below, in the United States mail at Los Angeles County, California, following standard court practices.

8/31/20  
DATED AND DEPOSITED

SHERRI R. CARTER, Executive Officer/Clerk

By: S. HUMBER, CLERK

Alan J. JACKSON, ESQ.  
KELLY C. QUINN, ESQ.  
MEHRUNISA RANJHA, ESQ.  
WERKSMAN JACKSON & QUINN LLP  
888 WEST SIXTH STREET, FOURTH FLOOR  
LOS ANGELES, CA. 90017

RAYMOND J. FUENTES, ESQ.  
JOHN L. FUENTES, ESQ.  
FUENTES & MCNALLY, LLP  
700 NORTH CENTRAL AVENUE, SUITE 450  
GLENDALE, CA. 91203-2602

No. 19-4172

---

**IN THE UNITED STATES COURT OF  
APPEALS FOR THE FOURTH CIRCUIT**

---

UNITED STATES OF AMERICA,

*Plaintiff–Appellee,*

v.

JAMES TIMOTHY COBB,

*Defendant–Appellant.*

On Appeal from the United States District  
Court for the Northern District of West  
Virginia, Clarksburg

Case No. 1:18-cr-00033-IMK-MJA

---

**BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION &  
AMERICAN CIVIL LIBERTIES UNION OF WEST VIRGINIA  
IN SUPPORT OF APPELLANT**

---

Nathan Freed Wessler  
Brett Max Kaufman  
Ezekiel Edwards  
Jason D. Williamson  
ACLU Foundation  
125 Broad St., 18th Floor  
New York, NY 10004  
212.549.2500  
nwessler@aclu.org

Jennifer Granick  
ACLU Foundation  
39 Drumm St.  
San Francisco, CA 94111  
415.621.2493  
jgranick@aclu.org

Loree Stark  
ACLU of West Virginia  
Foundation  
P.O. Box 3952  
Charleston, WV 25339  
304.345.9246  
lstark@acluwv.org



4. Is there any other publicly held corporation or other publicly held entity that has a direct financial interest in the outcome of the litigation (Local Rule 26.1(a)(2)(B))?  YES  NO  
If yes, identify entity and nature of interest:

5. Is party a trade association? (amici curiae do not complete this question)  YES  NO  
If yes, identify any publicly held member whose stock or equity value could be affected substantially by the outcome of the proceeding or whose claims the trade association is pursuing in a representative capacity, or state that there is no such member:

6. Does this case arise out of a bankruptcy proceeding?  YES  NO  
If yes, identify any trustee and the members of any creditors' committee:

Signature: /s/ Nathan Freed Wessler

Date: July 15, 2019

Counsel for: Amici

**CERTIFICATE OF SERVICE**

\*\*\*\*\*

I certify that on July 15, 2019 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

/s/ Nathan Freed Wessler  
(signature)

July 15, 2019  
(date)

## TABLE OF CONTENTS

TABLE OF AUTHORITIES .....	ii
STATEMENT OF INTERESTS OF AMICI.....	1
INTRODUCTION .....	2
ARGUMENT .....	3
I. Warrants to search digital devices must be circumscribed by search protocols or other limitations to ensure that they do not become unconstitutional general warrants.....	3
A. Searches must be limited to materials for which there is probable cause. ....	3
B. Electronic-device searches are challenging to execute because officers cannot readily tell which files are lawfully subject to search and seizure—but solutions are now available.....	5
II. With technology, courts can ensure that searches of digital devices are particularized, comprehensive, and reliable without investigators rummaging through every file. ....	8
A. Courts have met the challenges posed by searches of digital devices by circumscribing those searches in various ways to ensure Fourth Amendment compliance.....	8
B. Forensic tools enable law enforcement to conduct effective digital searches without rummaging through every file.....	12
III. The plain-view exception to the warrant requirement should not apply to indiscriminate digital searches. ....	16
A. Exceptions to the warrant requirement are strictly circumscribed by their own justifications and the strength .....	17
of government and private interests. ....	17
B. The traditional justifications for the plain-view doctrine—law-enforcement safety and evidence preservation—do not hold up in the context of highly invasive digital searches. ....	20
IV. This case illustrates why the plain-view exception should not apply when the government conducts an indiscriminate digital search.....	24
CONCLUSION .....	26

## TABLE OF AUTHORITIES

### Cases

<i>Andresen v. Maryland</i> , 427 U.S. 463 (1976) .....	4
<i>Arizona v. Gant</i> , 556 U.S. 332 (2009) .....	16, 17, 19
<i>Arizona v. Hicks</i> , 480 U.S. 321 (1987) .....	21
<i>Berger v. New York</i> , 388 U.S. 56 (1967) .....	4
<i>Carpenter v. United States</i> , 138 S. Ct. 2206 (2018).....	4, 17, 18, 19
<i>Collins v. Virginia</i> , 138 S. Ct. 1663 (2018).....	17, 19
<i>Coolidge v. New Hampshire</i> , 403 U.S. 443 (1971) .....	3, 16, 21, 23
<i>Ferguson v. City of Charleston</i> , 532 U.S. 67 (2001) .....	5
<i>Horton v. California</i> , 496 U.S. 128 (1990) .....	6, 23
<i>In re [REDACTED]@gmail.com</i> , 62 F. Supp. 3d 1100 (N.D. Cal. 2014).....	10
<i>In re Appeal of Application for Search Warrant</i> , 71 A.3d 1158 (Vt. 2012).....	7, 10
<i>In re Search of Info. Associated with Email Addresses Stored at Premises Controlled by Microsoft Corp.</i> , 212 F. Supp. 3d 1023 (D. Kan. 2016) .....	10

*Katz v. United States*,  
389 U.S. 347 (1967) .....16

*Ker v. California*,  
374 U.S. 23 (1963) .....21

*Riley v. California*,  
573 U.S. 373 (2014) ..... passim

*Stanford v. Texas*,  
379 U.S. 476 (1965) .....4

*United States v. Adjani*,  
452 F.3d 1140 (9th Cir. 2006) .....14

*United States v. Bishop*,  
338 F.3d 623 (6th Cir. 2003) .....22

*United States v. Burgess*,  
576 F.3d 1078 (10th Cir. 2009) .....10

*United States v. Comprehensive Drug Testing, Inc.*,  
621 F.3d 1162 (9th Cir. 2010) (en banc) ..... passim

*United States v. Galpin*,  
720 F.3d 436 (2d Cir. 2013) .....6

*United States v. Ganas*,  
824 F.3d 199 (2d Cir. 2016) (en banc) .....23

*United States v. Hill*,  
322 F. Supp. 2d 1081 (C.D. Cal. 2004) .....6

*United States v. Jackson*,  
131 F.3d 1104 (4th Cir. 1997) .....21

*United States v. Jacobsen*,  
466 U.S. 109 (1984) .....21

*United States v. Jeffers*,  
342 U.S. 48 (1951) .....17

*United States v. Kim*,  
103 F. Supp. 3d 32 (D.D.C. 2015).....20

*United States v. Kolsuz*,  
890 F.3d 133 (4th Cir. 2018) ..... 19, 20

*United States v. Riccardi*,  
405 F.3d 852 (10th Cir. 2005) .....10

*United States v. Sifuentes*,  
504 F.2d 845 (4th Cir. 1974) .....23

*United States v. Stetkiw*,  
No. 18-20579, 2019 WL 2866516 (E.D. Mich. July 3, 2019) ..... 11, 26

*United States v. Warshak*,  
631 F.3d 266 (6th Cir. 2010) .....5

*United States v. Williams*,  
592 F.3d 511 (4th Cir. 2010) .....7, 15

*United States v. Robinson*,  
275 F.3d 371 (4th Cir. 2001) .....4

*Washington v. Chrisman*,  
455 U.S. 1 (1982) .....21

**Statutes**

U.S. Const. amend. IV .....3

**Other Authorities**

AccessData, Forensic Toolkit User Guide (2017)..... 14, 15

Christina M. Schuck, Note, *A Search for the Caselaw to Support the Computer Search “Guidance” in United States v. Comprehensive Drug Testing*, 16 Lewis & Clark L. Rev. 741 (2012) .....23

Computer Crime & Intellectual Prop. Section, Crim. Div.,  
U.S. Dep’t of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009).....14

David H. Angeli & Christina M. Schuck, <i>The Plain View Doctrine and Computer Searches: Balancing Law Enforcement’s Investigatory Needs with Privacy Rights in the Digital Age</i> , 34 <i>Champion</i> 18 (Aug. 2010).....	22
Emily Berman, <i>Digital Searches, the Fourth Amendment, and the Magistrates’ Revolt</i> , 68 <i>Emory L.J.</i> 49 (2018).....	11
Guidance Software, <i>EnCase Forensic User Guide Version 8.07</i> (2018).....	13, 14
Karen Kent et al. <i>Guide to Integrating Forensic Techniques Into Incident Response: Recommendations of the Nat’l Inst. of Standards &amp; Tech.</i> (Nat’l Inst. of Standards & Tech., Tech. Admin., U.S. Dep’t of Commerce, No. 800-86, Aug. 2006).....	13
Madiyah Saudi, <i>An Overview of Disk Imaging Tool in Computer Forensics</i> (SANS Institute 2019) .....	12
Orin S. Kerr, <i>Searches and Seizures in a Digital World</i> , 119 <i>Harv. L. Rev.</i> 531 (2005).....	5, 14

## STATEMENT OF INTERESTS OF AMICI<sup>1</sup>

The American Civil Liberties Union (“ACLU”) is a nationwide, nonprofit, nonpartisan organization with more than two million members and supporters dedicated to the principles of liberty and equality embodied in the Constitution and our nation’s civil rights laws. Since its founding in 1920, the ACLU has frequently appeared before the Supreme Court and other federal courts in numerous cases implicating Americans’ right to privacy in the digital age, including as counsel in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and as amicus in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

The ACLU of West Virginia is a non-profit corporation dedicated to advancing civil liberties in West Virginia; it is an affiliate of the ACLU. Like the national organization, the ACLU of West Virginia has a long-time interest in protecting West Virginians’ rights to privacy.<sup>2</sup>

---

<sup>1</sup> All parties consent to the filing of this brief. No party or party’s counsel authored this brief or contributed money to fund the preparation or submission of this brief. No person other than amici, their members, and their counsel contributed money to fund the preparation or submission of this brief.

<sup>2</sup> Amici would like to thank Alexander Koster, a former student in the Advanced Technology Law & Policy Clinic at NYU School of Law, for his significant contributions to this brief.

## INTRODUCTION

Every day, law enforcement agents obtain and execute search warrants for digital materials stored on desktop computers, laptops, and cell phones. The information stored on these devices is vast, diverse, and far more sensitive than information stored in a filing cabinet, or even an entire home. Nevertheless, the court below held that when there is probable cause to search a device for evidence of one crime, the investigator may randomly open any or all other digital files stored on the device. This rule would transform every warrant to search an electronic device into a general warrant, allowing investigators to peruse potentially huge quantities of private material entirely unrelated to the factual predicate for a particular investigation.

Fortunately, there are more reasonable means of conducting digital searches without eviscerating the Fourth Amendment, including by imposing *ex ante* search protocols, using forensic search tools that protect non-responsive information from human eyes, using independent third party search teams, or simply by establishing in advance that the government may only retain or use material that is actually responsive to a warrant.

Because the computer search in this case was the digital equivalent of a general search, the Court should find it unconstitutional and should provide much-

needed guidance to lower courts about how to authorize and oversee electronic devices searches consistent with the Fourth Amendment.

## ARGUMENT

### **I. Warrants to search digital devices must be circumscribed by search protocols or other limitations to ensure that they do not become unconstitutional general warrants.**

Indiscriminate searches of hard drives and other electronic storage media, even if conducted pursuant to a warrant, violate the Fourth Amendment. Like other searches, electronic-device searches must be particularized—that is, cabined to files and folders for which the affidavit in support of the warrant provides probable cause. A contrary rule would give investigating officers a free hand to examine any and all files on a hard drive, merely because some files may be subject to search. That would upend the longstanding constitutional baseline rule that searches must be particularized and cannot constitute generalized rummaging through personal and private materials.

#### **A. Searches must be limited to materials for which there is probable cause.**

In order to comply with the Fourth Amendment, a search warrant must “particularly describ[e] the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. The particularity requirement of the Fourth Amendment is designed to ensure that those “searches deemed necessary should be as limited as possible.” *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971).

Constitutional searches must not consist of “a general, exploratory rummaging in a person’s belongings.” *United States v. Robinson*, 275 F.3d 371, 381 (4th Cir. 2001) (citing *Andresen v. Maryland*, 427 U.S. 463, 480 (1976)).

The particularity requirement is even more important when the privacy interests in the place to be searched are highly sensitive. In *Stanford v. Texas*, for example, the Supreme Court explained that “the constitutional requirement that warrants must particularly describe the ‘things to be seized’ is to be accorded the most scrupulous exactitude when the ‘things’ are books, and the basis for their seizure is the ideas which they contain.” 379 U.S. 476, 511–12 (1965). In *Berger v. New York*, the Supreme Court similarly stated that the need for particularity “is especially great in the case of eavesdropping” because such surveillance “involves an intrusion on privacy that is broad in scope.” 388 U.S. 41, 56 (1967).

Searches of digital information differ from physical-world searches in critical ways. See *Riley v. California*, 573 U.S. 373, 394–95 (2014); *Carpenter v. United States*, 138 S. Ct. 2206, 2217–18 (2018). Such searches threaten to intrude on protected privacy and property interests even more severely than electronic eavesdropping or searches of books and other written materials.

For one, computers contain far *more* information of an extremely personal nature than even the most capacious filing cabinet ever could. See *Riley*, 573 U.S. at 394–95; see also *United States v. Comprehensive Drug Testing, Inc. (CDT)*, 621

F.3d 1162, 1175 (9th Cir. 2010) (en banc) (per curiam); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 542 (2005).<sup>3</sup> Further, new *kinds* of data are stored in digital format that can reveal extraordinarily sensitive information. Many categories of information that courts have recognized as deserving of particularly stringent privacy protections can be contained on people’s electronic devices, including internet browsing history, medical records, email, privileged communications, and associational information. *See, e.g., Riley*, 573 U.S. at 395; *Ferguson v. City of Charleston*, 532 U.S. 67, 78 (2001); *United States v. Warshak*, 631 F.3d 266, 286 (6th Cir. 2010). Indeed, the search of such devices “would typically expose to the government far more than the most exhaustive search of a house,” not least because they “contain[] a broad array of private information *never* found in a home in any form” prior to the digital age. *Riley*, 573 U.S. at 396–97.

**B. Electronic-device searches are challenging to execute because officers cannot readily tell which files are lawfully subject to search and seizure—but solutions are now available.**

Digital searches require strict adherence to the Fourth Amendment’s particularity requirement in order to avoid unconstitutional rummaging through private materials. To be sure, meeting this requirement can be challenging. Yet

---

<sup>3</sup> Laptops sold in 2019 can store up to four terabytes of information, the equivalent of more than 2.5 billion pages of text. *See, e.g.,* Apple, Compare Mac Models, <https://perma.cc/2LT8-FN3B>; LexisNexis, *How Many Pages in a Gigabyte* (2007), <https://perma.cc/HN26-3ZVC>.

courts and investigators have effective tools at their disposal to comply with the Fourth Amendment's command.

In the physical world, searches generally are readily particularized by the practical characteristics of the things and places for which there is probable cause. For example, officers are easily restricted to looking in only those places large enough to hold the physical items particularly described in the warrant. Police cannot open a spice box when searching for a rifle. *See, e.g., Horton v. California*, 496 U.S. 128, 141 (1990). Nor can they rummage through a medicine cabinet to look for a flat-screen television. *See, e.g., United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013).

However, this common-sense limit is much more difficult to apply in the digital realm. Digital data for which there is probable cause may, to a human eye, look more or less the same as non-responsive off-limits information. For example, a word-processing document might contain text, images, or both—but a human observer may not readily anticipate which before opening the file. Similarly, the size of an electronic file has little bearing on the file's contents. *See id.* at 447; *United States v. Hill*, 322 F. Supp. 2d 1081, 1090–91 (C.D. Cal. 2004) (Kozinski, J.) (“There is no way to know what is in a file without examining its contents, just as there is no sure way of separating talcum from cocaine except by testing it.”), *aff'd* 459 F.3d 966 (9th Cir. 2006).

In light of this challenge, this Court in *United States v. Williams*, 592 F.3d 511, 521 (4th Cir. 2010), and the district court below, JA246, have suggested that officers have little choice but to rummage through any or all digitally stored materials to look for evidence of the crime under investigation—thereby exposing an enormous variety of private data to expansive searches and seizures. But the assumptions underlying this conclusion nearly a decade ago in *Williams* have been undermined by subsequent technological and legal developments.

First, courts now have more experience imposing search protocols or other limitations to circumscribe digital searches, thus preventing overbroad searches that would “render[]the Fourth Amendment irrelevant.” *CDT*, 621 F.3d at 1168–69, 1176 (per curiam); *see also, e.g., id.* at 1179 (Kozinski, C.J., concurring) (detailing digital search protocols); *In re Appeal of Application for Search Warrant*, 71 A.3d 1158 (Vt. 2012) (same). *See infra* Part II.A.

And second, technology has changed since this Court’s opinion in *Williams*. If it were ever true, it is no longer the case that in executing warrants for searches of digital information, investigators sometimes must manually “open each file on the computer and view its contents, at least cursorily, to determine whether the file [falls] within the scope of the warrant’s authorization.” *Williams*, 592 F.3d at 521. Today, there are readily available forensic tools that (1) do a better job of searching for information than a human review can; (2) do a better job of protecting the

privacy of non-responsive information; and (3) do a better job of ensuring that evidence seized has not been tampered with or altered in the course of an investigation. *See infra* Part II.B.

**II. With technology, courts can ensure that searches of digital devices are particularized, comprehensive, and reliable without investigators rummaging through every file.**

**A. Courts have met the challenges posed by searches of digital devices by circumscribing those searches in various ways to ensure Fourth Amendment compliance.**

There is a growing judicial recognition that courts must impose limits on digital searches—for example, via *ex ante* search protocols—to ensure Fourth Amendment protections for highly sensitive digital information. Many courts have suggested limits above and beyond those imposed on traditional physical-world searches. These limits nevertheless permit law enforcement to conduct effective investigations, but without unreasonable invasions of privacy.

For example, the *en banc* Ninth Circuit has recognized that the digital age calls for “greater vigilance on the part of judicial officers in striking the right balance between” law-enforcement interests and privacy, and in ensuring that digital searches do “not become a vehicle for the government to gain access to data which it has no probable cause to collect.” *CDT*, 621 F.3d at 1177 (per curiam).<sup>4</sup>

---

<sup>4</sup> In *CDT*, the government obtained a warrant to search the electronically-stored drug-testing records of ten Major League Baseball players. 621 F.3d at 1166 (per curiam). When executing the warrant, however, agents examined the drug-testing

The various opinions in *CDT* proposed a menu of potential solutions in the form of *ex ante* search protocols, without which magistrates should deny search warrants for digital data. *See id.* at 1179–80 (Kozinski, C.J., concurring) (“summ[ing] up” the court’s guidance).

One option is to require the use of independent review teams to “sort[], segregat[e], decod[e] and otherwise separat[e] seizable data (as defined by the warrant) from all other data,” so as to shield investigators from exposure to information beyond the scope of the warrant. *Id.* at 1179; *see id.* at 1168–72 (per curiam). Another is to require the use of technology, including “hashing tools,” to identify responsive files “without actually opening the files themselves.” *Id.* at 1179 (Kozinski, C.J., concurring). And yet another is to “waive reliance upon the plain view doctrine in digital evidence cases,” full stop—in other words, to agree not to take advantage of the government’s unwillingness or inability to conduct digital searches in a particularized manner. *Id.* at 1180; *see id.* at 1170–71 (per curiam). Regardless of the method chosen, however, it “must be designed to uncover only the information for which it has probable cause, and only that information may be examined by the case agents.” *Id.* at 1180 (Kozinski, C.J., concurring).

---

records of hundreds of other players whose files were intermingled with those of the ten players named in the warrant. *Id.*

Courts now regularly implement versions of these solutions. For example, in Vermont, magistrates may design and supervise “targeted searches” by “restricting law enforcement’s search to those items that met certain parameters based on dates, types of files, or the author of a document.” *See In re Search Warrant*, 71 A.3d at 1184. Similarly, the Tenth Circuit requires that computer search warrants affirmatively limit the search to evidence of specific federal crimes or specific types of material, and investigators are prohibited from indiscriminately opening every file on a hard drive. *See United States v. Riccardi*, 405 F.3d 852, 862 (10th Cir. 2005); *United States v. Burgess*, 576 F.3d 1078, 1091 (10th Cir. 2009) (“If the warrant is read to allow a search of all computer records without description or limitation it would not meet the Fourth Amendment’s particularity requirement.”). Other courts have similarly held that, under the Fourth Amendment’s particularity requirement, law enforcement may need to use date-range restrictions, or other limitations, to prevent the potential for “general rummaging” when searching electronically stored information such as email accounts. *See, e.g., In re Search of Info. Associated with Email Addresses Stored at Premises Controlled by Microsoft Corp.*, 212 F. Supp. 3d 1023, 1037 (D. Kan. 2016); *In re [REDACTED]@gmail.com*, 62 F. Supp. 3d 1100, 1104 (N.D. Cal. 2014) (denying a search warrant for a particular email account because “there [was] no date restriction of any kind”).

A recent district court case from Michigan helpfully illustrates how courts are now confronting these issues. In *United States v. Stetkiw*, the government insisted, and the court was concerned, that, “individuals might hide information in a way that forces a protocol-bound investigator to overlook it.” No. 18-20579, 2019 WL 2866516, at \*5 (E.D. Mich. July 3, 2019) (Roberts, J.). Nevertheless, the court held that “an *ex ante* ‘minimization’ requirement can address concerns about potential Fourth Amendment violations of protocol-less searches, with a goal of decreasing the amount of non-responsive [electronically stored information] encountered in a search.” *Id.* (citing Emily Berman, *Digital Searches, the Fourth Amendment, and the Magistrates’ Revolt*, 68 Emory L.J. 49, 55 (2018)). The court concluded that *ex ante* procedures would have several advantages: they would minimize contentious *ex post* review in the suppression context; they would allow for case-by-case tailoring of warrants to uncover materials whose seizure is supported by probable cause; they would permit judicial conversation over appropriate limitations; and they would help prevent even inadvertent conversions of warrants into general warrants. *See id.* While the *Stetkiw* court did not maintain that *ex ante* protocols must be required in every case, it did suggest that in order to escape such protocols, the government “should demonstrate that the level of probable cause to search [electronically stored information] is high enough to justify a search without minimization.” *Id.*

**B. Forensic tools enable law enforcement to conduct effective digital searches without rummaging through every file.**

Requiring law enforcement to perform particularized digital searches will not interfere with legitimate investigations. Today's forensic tools enable law enforcement (or independent "clean teams") to efficiently and effectively conduct comprehensive hard drive searches, sifting out responsive material from other data, without a human looking at every file.

It is true that computer files are easy to disguise or rename. It is also true that evidence may be not only contained in an electronic file, but also in volatile memory, configuration files, or operating system data. Contrary to common assumptions (and government claims), however, these facts do not require investigators to open every file in order to locate the evidence to which the government is entitled through a search warrant. In fact, comprehensive human review can often be counterproductive or incomplete. For example, a human does not have enough time to search every file, and rummaging does not reveal evidence that may be hiding in these other forms of storage. Further, randomly opening files (as the investigator did in this case) may alter the data on the machine, risking accidental spoliation or obfuscation. *See* Madihah Saudi, *An Overview of Disk Imaging Tool in Computer Forensics* § 5.1 (SANS Institute 2019), <https://perma.cc/P7QK-7WPQ> ("One of the cardinal rules in computer forensics is never work on the original evidence."); Karen Kent et al. *Guide to*

*Integrating Forensic Techniques Into Incident Response: Recommendations of the Nat'l Inst. of Standards & Tech.* (Nat'l Inst. of Standards & Tech., Tech. Admin., U.S. Dep't of Commerce, No. 800-86, Aug. 2006), <https://perma.cc/Y2N7-K65R>.

Forensic software, on the other hand, offers law enforcement a tool for running particularized digital searches—that is, searches that are designed to reveal files and folders for which a warrant establishes probable cause. To be clear, in many cases, forensic software technically *searches* every file as well as other data stored on a hard drive. But the search is more *reasonable* because it becomes far less likely that non-responsive data will be exposed to investigators.

For example, EnCase Forensic Software (“EnCase”) is a law enforcement search tool for hard drives and mobile devices. EnCase can be configured to search for specific files or types of data on the computer—such as emails, internet searches,<sup>5</sup> photographs,<sup>6</sup> documents,<sup>7</sup> files over a specified size,<sup>8</sup> files with a particular extension,<sup>9</sup> files containing personal identifying information (such as email addresses and credit card, Social Security, and phone numbers),<sup>10</sup> or files

---

<sup>5</sup> Guidance Software, EnCase Forensic User Guide Version 8.07, at 64–65 (2018), <https://perma.cc/NN95-ZNPM>.

<sup>6</sup> *Id.* at 62.

<sup>7</sup> *Id.*

<sup>8</sup> *Id.*

<sup>9</sup> *Id.*

<sup>10</sup> *Id.* at 338.

containing certain keywords.<sup>11</sup> Law enforcement widely uses these forensic tools because they search regardless of how the information is stored or named. For example, while file extension search filters are imperfect (since a suspect could disguise a photo by resaving a “.jpg” to a “.doc” extension),<sup>12</sup> “file header” functionalities on EnCase can determine a file’s format regardless of filename or extension.<sup>13</sup> Forensic software programs can also detect embedded file images—that is, photographs hidden inside of Microsoft Word documents.<sup>14</sup> And while keyword searches can be imperfect,<sup>15</sup> today Optical Character Recognition (“OCR”)—a common forensic tool that automatically extracts text contained in graphic files, such as images or non-searchable PDFs—addresses that challenge.<sup>16</sup>

The tools also perform targeted searches, which enable investigators to comprehensively and efficiently home in on the digital evidence most likely to be

---

<sup>11</sup> *Id.* at 143, 246.

<sup>12</sup> Computer Crime & Intellectual Prop. Section, Crim. Div., U.S. Dep’t of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 36 (2009), <https://perma.cc/VP23-RZTJ> (“DOJ Manual”) (quoting *United States v. Adjani*, 452 F.3d 1140, 1150 (9th Cir. 2006)).

<sup>13</sup> Kerr, 119 Harv. L. Rev. at 545.

<sup>14</sup> *See, e.g.*, AccessData, Forensic Toolkit User Guide 139 (2017), <https://perma.cc/E5KY-F6LY> (“FTK User Guide”) (“To recover embedded or deleted files, the case evidence is searched for specific file headers. . . . Embedded or deleted items can be found as long as the file header still exists.”).

<sup>15</sup> DOJ Manual at 79.

<sup>16</sup> FTK User Guide at 95 (“The [OCR] process lets you extract text that is contained in graphics files. The text is then indexed so that it can be[] searched[] and bookmarked.”).

warrant-responsive, while ignoring other information. Investigators can limit a search to a particular date range, allowing analysts to obtain files within temporal proximity of the relevant crime.<sup>17</sup> EnCase can automatically identify illegal files (such as child pornography) without a human investigator needing to open the file. Similar tools include Forensic ToolKit and Cellebrite. There are many such products on the market and available to law enforcement at the state and local level as well as to the FBI.

These facts call into question the district court's claim that there was a need to randomly open up files on the defendant's laptop to determine which files were authorized for seizure. JA247. Forensic software could conduct a more thorough search without altering the data on the original hard drive or disclosing non-responsive information to the officer.<sup>18</sup> These facts also explain why older case law, like *Williams*, 592 F.3d at 521, does not dictate the outcome here: that decision was premised on the unavailability of modern forensic tools that are widely used today. Technology has exacerbated the danger of general searches in the digital realm, but it may also be used to ensure that those searches comply with the Fourth Amendment going forward.

---

<sup>17</sup> *Id.* at 102.

<sup>18</sup> Indeed, the investigators in this matter had access to the state police digital lab in Morgantown, which employs “[s]ome kind of forensic tool” that eventually was used to more comprehensively examine the seized hard drive. JA129.

**III. The plain-view exception to the warrant requirement should not apply to indiscriminate digital searches.**

The use of *ex ante* search protocols imposed by a magistrate—whether they be assignment to “clean teams,” targeted search protocols, or the use of forensic tools—would be the preferred approach in most cases. But where police do not adopt such methods, courts should firmly reject application of the “plain view” exception to the Fourth Amendment’s warrant requirement.

“[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions.” *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)). Among those exceptions is “plain view.” *See, e.g., Coolidge*, 403 U.S. 443. The plain-view exception developed in cases concerning physical-world searches, permitting the government to obtain evidence not covered by a warrant where law enforcement discovered it in the course of a lawfully authorized search. However, the application of the plain-view exception does not make sense in the context of highly invasive searches of laptops, hard drives, and other electronically stored information.

**A. Exceptions to the warrant requirement are strictly circumscribed by their own justifications and the strength of government and private interests.**

Exceptions to the warrant requirement do not apply automatically upon invocation; rather, they must remain “[tether[ed]]” to “the justifications underlying the . . . exception.” *Gant*, 556 U.S. at 343. The government bears the burden of demonstrating that an exception to the warrant requirement ought to apply in a given context. *United States v. Jeffers*, 342 U.S. 48, 51 (1951). As the Supreme Court recently explained, this analysis requires courts to “assess[] on the one hand, the degree to which it intrudes upon an individual’s privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.” *Riley*, 573 U.S. at 385. Time and time again, the Supreme Court has refused to “unmoor [warrant] exception[s] from [their] justifications . . . and transform what was meant to be an exception into a tool with far broader application.” *Collins v. Virginia*, 138 S. Ct. 1663, 1672–73 (2018). Thus, the Supreme Court has chosen not to apply even well-recognized warrant exceptions where the underlying rationale for an exception is absent from a given fact pattern.

This is particularly so when courts are asked to apply analog-era exceptions to new digital contexts. *See, e.g., Riley*, 573 U.S. at 393; *Carpenter*, 138 S. Ct. at 2222. In *Riley*, the Court declined to extend the search-incident-to-arrest exception developed in cases involving arrestees’ possession of items like cigarette packs to

the digital information contained on an arrestee’s cell phone. There, the government “assert[ed] that a search of all data stored on a cell phone [was] ‘materially indistinguishable’ from searches of . . . physical items,” but the Court issued a harsh rejoinder:

That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together. Modern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse. A conclusion that inspecting the contents of an arrestee’s pockets works no substantial additional intrusion on privacy beyond the arrest itself may make sense as applied to physical items, but any extension of that reasoning to digital data has to rest on its own bottom.

573 U.S. at 393. Holding otherwise would have “untether[ed] the rule from the justifications underlying the [search-incident-to-arrest] exception”—that is, officer safety and evidence preservation. *Id.* at 386.

Similarly, in *Carpenter*, the Court rejected the government’s invocation of the “third-party doctrine”—an exception to normal Fourth Amendment protections based on individuals’ supposedly reduced expectation of privacy in information shared with others—to justify warrantless collection of digital location information held by phone companies. *See* 138 S. Ct. at 2219–22. The Court explained that the “Government’s position fails to contend with the seismic shifts in digital technology” that untethered the traditional rationale for the third-party doctrine

from its application to an “exhaustive chronicle of location information casually collected by wireless carriers.” *Id.* at 2219.

The Supreme Court has limited other warrant exceptions to their justifications as well. In *Gant*, for example, the Court declined to extend the search-incident-to-arrest exception to the warrantless search of a passenger compartment in defendant-arrestee’s vehicle where “unnecessary to protect law enforcement safety and evidentiary interests.” 556 U.S. at 346. In *Collins v. Virginia*, the Court held that the automobile exception does not allow an officer to enter a home or its curtilage without a warrant because, unlike vehicles, the curtilage of a home is not readily mobile. 138 S. Ct. at 1672–73. And in *City of Los Angeles v. Patel*, the Court declined to apply the exception for closely regulated industries to warrantless searches of hotel guest registries because, unlike inherently dangerous industries with a history of government oversight such that no proprietor could have a reasonable expectation of privacy, “nothing inherent in the operation of hotels poses a clear and significant risk to the public welfare.” 135 S. Ct. 2443, 2454 (2015).

Similarly, this Court recently declared in *United States v. Kolsuz*, that “[a]s a general rule, the scope of a warrant exception should be defined by its justifications.” 890 F.3d 133, 143 (4th Cir. 2018) (citing *Riley*, 573 U.S. at 385–91). The Court further explained that—particularly when it comes to digital-age

searches—“where the government interests underlying a Fourth Amendment exception are not implicated by a certain type of search, and where the individual’s privacy interests outweigh any ancillary governmental interests, the government must obtain a warrant based on probable cause.” *Id.* As a result, in *Kolsuz*, the Court had little trouble rejecting the government’s argument that the “border search exception,” which is “justified by the government’s power to regulate the export of currency and other goods,” including “dangerous weapons,” permits invasive, suspicionless searches of travelers’ electronic devices conducted at a national border. *Id.* at 138. Other courts have performed similar analyses. *See, e.g., United States v. Kim*, 103 F. Supp. 3d 32, 59 (D.D.C. 2015) (refusing to extend border-search exception to warrantless search of laptop computer).

**B. The traditional justifications for the plain-view doctrine—law-enforcement safety and evidence preservation—do not hold up in the context of highly invasive digital searches.**

As the Supreme Court explained in *Riley*, courts considering whether to “exempt a given type of search from the warrant requirement” must balance “the degree to which [the search] intrudes upon an individual’s privacy” against “the degree to which it is needed for the promotion of legitimate governmental interests.” 573 U.S. at 385. As discussed above, there is an enormous (and growing) privacy interest in electronic devices like laptop computers and cell phones. *See supra* Part I.A; *Riley*, 573 U.S. at 393–98. On the other hand, the

government interest justifying the plain-view exception is “the desirability of sparing police . . . the inconvenience and the risk—to themselves or to preservation of the evidence—of going to obtain a warrant.” *Arizona v. Hicks*, 480 U.S. 321, 326–27 (1987) (citing *Coolidge*, 403 U.S. at 467–68). Applying plain view to excuse a warrantless search may make good sense where delay caused by obtaining a warrant could lead to evidence spoliation. *See, e.g., Washington v. Chrisman*, 455 U.S. 1, 9 (1982); *Ker v. California*, 374 U.S. 23, 42 (1963). But a plain-view argument fails where the interests served by the application of the exception are outweighed by the privacy interests involved. *See, e.g., Coolidge*, 403 U.S. at 472.

The justifications underlying plain view—evidence preservation and officer safety—are at their apex in relation to seizures, but not necessarily searches. *United States v. Jacobsen*, 466 U.S. 109, 114 (1984) (“Even when government agents may lawfully seize such a package to prevent loss or destruction of suspected contraband, the Fourth Amendment requires that they obtain a warrant before examining the contents of such a package.”). This Court has been even more categorical, explaining that “[t]he ‘plain-view’ doctrine provides an exception to the warrant requirement for the *seizure* of property, but it does not provide an exception for a search.” *United States v. Jackson*, 131 F.3d 1104, 1108 (4th Cir. 1997).

The plain-view doctrine developed in cases involving physical-world searches, where evidence is tangible and discrete, but searches of digital information are a poor fit for the plain-view exception because the justifications underlying the exception are, by and large, absent in this context. First, officer safety is not implicated in a controlled environment like an off-site forensics laboratory. *See generally* David H. Angeli & Christina M. Schuck, *The Plain View Doctrine and Computer Searches: Balancing Law Enforcement’s Investigatory Needs with Privacy Rights in the Digital Age*, 34 *Champion* 18, 23 (Aug. 2010). Unlike a physical object, such as a knife or gun, *see, e.g., United States v. Bishop*, 338 F.3d 623, 628–29 (6th Cir. 2003), the digital data stored on a computer hard drive can physically endanger no one. *See Riley*, 573 U.S. at 386–87. Second, evidence preservation is not at risk in a typical computer search, which normally begins with the creation of a “bitstream” copy of the target hard drive.<sup>19</sup> Third, where the computer hard drive is preserved pending execution of the warrant, the police have ample time to obtain additional warrants (say, for evidence of an unrelated crime) without risking evidence destruction. *See, e.g.,* Christina M. Schuck, Note, *A Search for the Caselaw to Support the Computer Search*

---

<sup>19</sup> Kerr, 119 *Harv. L. Rev.* at 540.

“*Guidance*” in *United States v. Comprehensive Drug Testing*, 16 Lewis & Clark L. Rev. 741, 760–61 (2012).<sup>20</sup>

In order to apply plain view, first, law enforcement’s observation of the plain-view evidence must have taken place after an initially lawful intrusion (based on, for example, an existing warrant or exigency). *See United States v. Sifuentes*, 504 F.2d 845, 848 (4th Cir. 1974) (citing *Coolidge*, 403 U.S. at 466). Second, the evidence and its incriminating character must be “obvious to the senses”—that is, there for the seeing, out in the open, rather than obscured or hidden. *See id.* Moreover, the discovery of the material will often (if not always) be inadvertent, rather than intentional. *See id.*; *Horton*, 496 U.S. at 130.

These conditions are not regularly met in the context of searches of digital information. First, a warrant to search for *some* material on a computer does not automatically entitle the government to review *all* of the material on that computer. *See supra* Part I.A. Second, the incriminating nature of digital evidence will not immediately be “obvious to the senses” because file types, names, and sizes do not necessarily reveal their contents. *See supra* Part I.B. And last, when the government opens files one by one, it knows that it will encounter non-responsive information for which there is no probable cause—which is hardly inadvertent.

---

<sup>20</sup> Of course, the government may not retain nonresponsive data beyond the time reasonably necessary to execute its warrant. *See, e.g., United States v. Ganius*, 824 F.3d 199, 226–41 (2d Cir. 2016) (en banc) (Chin, J., dissenting).

**IV. This case illustrates why the plain-view exception should not apply when the government conducts an indiscriminate digital search.**

The facts of this case show why permitting the government to rely on the plain-view exception to introduce evidence obtained through indiscriminate searches of digital information endangers the public’s constitutional rights.

First, officers were investigating a murder case and lacked any probable cause to search the defendant’s computer for child pornography. Nevertheless, the officer who searched Defendant’s computer for evidence related to the homicide admitted that he intended to search for evidence of crimes unrelated to the homicide. JA116, JA118, JA124. The officer’s decision to open files manually—a random, indiscriminate, and broad search method—enabled him to achieve his unconstitutional goal. *See also* JA40, JA113–14 (officer admitting that he uses the “[a]ny and all evidence of any other crimes” language in almost every search warrant for digital information); JA127 (officer “encountered” the pornographic photographs “just by going through the files”); JA128 (“I started clicking on some icons and the [pornographic] pictures came up and they were just there.”). At the suppression hearing, the officer testified that “you never know what you’re going to find.” JA118.

This officer effectively said out loud what silently lurks in many digital-search cases: “going through files” and “clicking on icons” converts even a facially

particularized warrant into an unconstitutional general warrant.<sup>21</sup> *See, e.g., CDT*, 621 F.3d at 1171 (per curiam) (“The government agents obviously were counting on the search to bring constitutionally protected data into the plain view of the investigating agents.”). The mere fact that this was a digital search should not enable an officer to deliberately rummage for evidence of “any and all crimes,” in violation of bedrock Fourth Amendment principles. *See supra* Part I.A.

Second, the perfunctory nature of the officer’s interaction with the magistrate in obtaining the second warrant illustrates how critical it is for courts like this one to ensure that magistrates require reasonable search protocols when authorizing digital searches. *See supra* Parts I.B, II.A. Here, the officer met with the magistrate—who was not familiar with the investigation, and did not ask the officer any questions—for five minutes before walking away with an approval. JA40–45, JA121–22. But as searches of digital information become more and more commonplace (and more and more capable of leading to deeply intrusive searches of material unrelated to the purposes of authorized searches), the supervisory role

---

<sup>21</sup> This would be a different case had the officer inadvertently discovered the child pornography as a result of a targeted search query designed to obtain only evidence of the homicide. Under those facts, the discovery of the contraband files might have fallen within the plain-view exception. However, other than searching for references to “suffocation”—the mechanism of injury in Mr. Wilson’s homicide—the officer did not employ targeted search techniques of any kind. JA126. Rather, as mentioned, his search method was random and indiscriminate. *Id.*

of independent magistrates will become more and more important. *See, e.g., Stetkiw*, 2019 WL 2866516, at \*5.

Third, neither of the justifications that underlie the traditional plain-view doctrine—evidence preservation nor officer safety—are relevant to this case. *See supra* Part III.B. Police had seized the defendant’s laptop and the investigation was concerned with motive rather than any ongoing crimes. JA110. The defendant was in custody. There was no exigency or continuing danger.

### CONCLUSION

For the reasons stated above, the evidence obtained after the investigator randomly opened files on the defendant’s computer should have been suppressed.

Date: July 15, 2019

/s/ Nathan Freed Wessler

Nathan Freed Wessler  
Brett Max Kaufman  
Ezekiel Edwards  
Jason D. Williamson  
ACLU Foundation  
125 Broad St., 18th Floor  
New York, NY 10004  
212.549.2500  
nwessler@aclu.org  
bkaufman@aclu.org

Jennifer Granick  
ACLU Foundation  
Speech, Privacy, and  
Technology Project  
39 Drumm St.  
San Francisco, CA 94111  
415.621.2493  
jgranick@aclu.org

Loree Stark  
ACLU of West Virginia  
Foundation  
P.O. Box 3952  
Charleston, WV 25339  
304.345.9246  
lstark@acluwv.org

**CERTIFICATE OF COMPLIANCE**

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify that:

This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 5,988 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionately spaced typeface using Times New Roman 14-point font.

Date: July 15, 2019

/s/ Nathan Freed Wessler  
Nathan Freed Wessler

*Counsel for Amici*

**CERTIFICATE OF SERVICE**

I hereby certify that on July 15, 2019, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Fourth Circuit by using the appellate CM/ECF system. Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

Date: July 15, 2019

/s/ Nathan Freed Wessler  
Nathan Freed Wessler

*Counsel for Amici*

UNITED STATES COURT OF APPEALS FOR THE FOURTH CIRCUIT
APPEARANCE OF COUNSEL FORM

BAR ADMISSION & ECF REGISTRATION: If you have not been admitted to practice before the Fourth Circuit, you must complete and return an Application for Admission before filing this form. If you were admitted to practice under a different name than you are now using, you must include your former name when completing this form so that we can locate you on the attorney roll. Electronic filing by counsel is required in all Fourth Circuit cases. If you have not registered as a Fourth Circuit ECF Filer, please complete the required steps at Register for eFiling.

THE CLERK WILL ENTER MY APPEARANCE IN APPEAL NO. 19-4172 as

[X] Retained [ ] Court-appointed(CJA) [ ] Court-assigned(non-CJA) [ ] Federal Defender [ ] Pro Bono [ ] Government

COUNSEL FOR: American Civil Liberties Union and American Civil Liberties Union of West

Virginia as the (party name)

[ ] appellant(s) [ ] appellee(s) [ ] petitioner(s) [ ] respondent(s) [X] amicus curiae [ ] intervenor(s) [ ] movant(s)

/s/ Nathan Freed Wessler (signature)

Please compare your information below with your information on PACER. Any updates or changes must be made through PACER's Manage My Account.

Nathan Freed Wessler Name (printed or typed)

(212) 549-2500 Voice Phone

American Civil Liberties Union Foundation Firm Name (if applicable)

(212) 549 -2654 Fax Number

125 Broad Street, 18th Floor

New York, NY 10004 Address

nwessler@aclu.org E-mail address (print or type)

CERTIFICATE OF SERVICE

I certify that on July 15, 2019 the foregoing document was served on all parties or their counsel of record through the CM/ECF system if they are registered users or, if they are not, by serving a true and correct copy at the addresses listed below:

[Empty box for address]

[Empty box for address]

/s/ Nathan Freed Wessler Signature

July 15, 2019 Date

**PUBLISHED**

UNITED STATES COURT OF APPEALS  
FOR THE FOURTH CIRCUIT

---

**No. 19-4172**

---

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

v.

JAMES TIMOTHY COBB,

Defendant - Appellant.

-----

AMERICAN CIVIL LIBERTIES UNION; AMERICAN CIVIL LIBERTIES  
UNION OF WEST VIRGINIA,

Amici Supporting Appellant.

---

Appeal from the United States District Court for the Northern District of West Virginia, at  
Clarksburg. Irene M. Keeley, Senior District Judge. (1:18-cr-00033-IMK-MJA-1)

---

Submitted: June 1, 2020

Decided: August 11, 2020

Amended: August 17, 2020

---

Before WILKINSON and FLOYD, Circuit Judges, and TRAXLER, Senior Circuit Judge.

---

Affirmed by published opinion. Senior Judge Traxler wrote the opinion, in which Judge  
Wilkinson joined. Judge Floyd wrote a dissenting opinion.

---

L. Richard Walker, Senior Litigator, Clarksburg, West Virginia, Kristen Leddy, Assistant Federal Public Defender, OFFICE OF THE FEDERAL PUBLIC DEFENDER, Martinsburg, West Virginia, for Appellant. William J. Powell, United States Attorney, Sarah E. Wagner, OFFICE OF THE UNITED STATES ATTORNEY, Clarksburg, West Virginia, for Appellee. Nathan Freed Wessler, Brett Max Kaufman, Ezekiel Edwards, Jason D. Williamson, New York, New York, Jennifer Granick, ACLU FOUNDATION, San Francisco, California; Loree Stark, ACLU OF WEST VIRGINIA FOUNDATION, Charleston, West Virginia, for Amici American Civil Liberties Union and American Civil Liberties Union of West Virginia

---

TRAXLER, Senior Circuit Judge:

Defendant James Timothy Cobb (“Cobb”) entered a conditional guilty plea to possession of child pornography. He appeals the district court’s denial of his motion to suppress the images that were seized from his computer pursuant to a search warrant issued by a state magistrate judge. For the following reasons, we affirm.

I.

On September 7, 2014, Cobb, who was 57 years old at the time, was living with his parents, James and Freda Cobb, and his cousin, Paul Dean Wilson, in Marion County, West Virginia. A fight broke out that evening between Cobb and Wilson. Cobb put Wilson in a chokehold and put his knee in Wilson’s chest. The fight was witnessed by Cobb’s parents, who called 911 for assistance. Wilson was unresponsive when police arrived, and he was pronounced dead at the scene by emergency medical personnel. Cobb was arrested and jailed that evening, charged with the second-degree murder of Wilson.

Unbeknownst to Cobb’s parents, the phone line remained open after the 911 calls were placed. The parents were recorded begging Cobb to stop, and telling Cobb that Wilson was “helpless,” and he was “going to end up killing the man.” J.A. 54. During questioning later by law enforcement, Cobb’s parents gave varying accounts of the events leading up to the murder. Cobb’s father said the fight started over Wilson’s firearm. The father also said that Wilson threatened him and his son stepped in to protect him. The mother, on the other hand, told the officers that Wilson punched her in the mouth because she yelled at him for being mean to his cat, and that her son was protecting her. In a recorded jail call on September 8, Cobb and his parents discussed the various versions of

the events. During the call, the mother told Cobb that she put cotton in her lip and took a picture, on the advice of a neighbor, to support her version.

On September 9, 2014, less than 48 hours after the murder, Cobb was recorded in another jail call telling his father to remove a laptop computer from the bed in Cobb's room and to "put it in his father's room 'to keep it safe.'" J.A. 163. Cobb told his father that "Wilson had previously used the computer and put some 'shit' on it," and Cobb requested that his father "'wipe down' or 'clean' the computer." J.A. 163. Cobb also told his parents to get his cell phone from the jail.

After consulting with the state prosecutor, the investigating officers obtained a search warrant to search Cobb's residence for "[a]ny and all firearms belonging to Paul Dean Wilson Jr., any and all laptop computers, including tablets or desktop computers belonging to or operated by James Timothy Cobb, any and all cell phones belonging to or operated by James Timothy Cobb, and any and all evidence of a crime." J.A. 36. The probable cause statement reads as follows:

On 09/07/14, at approx. 2355 hrs [d]eputies responded to an altercation at [Cobb's home]. Once on scene deputies advised that a male subject was unresponsive and started CPR. Once the undersigned arrived on scene the male subject, identified as Paul Dean Wilson Jr., was pronounced dead by EMTs. The undersigned then spoke with witnesses in the residence, James K. Cobb and Freda Cobb, who advised a physical altercation had taken place between James Timothy Cobb and his cousin Paul Dean Wilson Jr. During the altercation between James T. Cobb and Wilson, James T. Cobb placed Wilson in a choke hold and placed his knee on his chest and pulled his head towards his knee. . . . When deputies arrived on scene James T. Cobb still had Wilson restrained and Wilson was unresponsive. On 09/09/14 statements were made by James Timothy Cobb requesting his parents, James Keith Cobb and Freda Cobb, have a subject clean off his laptop and pick up his cellular telephone from the jail. Also upon speaking with James K. Cobb he advised that Paul Dean Wilson Jr. had possession of a hand gun he called

a “Beretta” and started the altercation over the firearm not being where Mr. Wilson left the gun. The above events occurred in Marion Co. WV.

J.A. 36, 38. The investigating officers executed the warrant and seized, among other things, three firearms and a Gateway laptop computer believed to be the computer that Cobb referred to in the phone call with his father.

On September 23, 2014, the officers obtained a second warrant to search the internal contents of the Gateway laptop computer for evidence of the murder. The probable cause statement included in this warrant reads as follows:

On September 7, 2014[,] the Marion County Sheriff’s Dept. responded to a domestic altercation between James Timothy Cobb and Paul Dean Wilson Jr. who are cousins both living with Cobb’s parents at [their residence] in Marion Co. Wilson was pronounced dead at the scene. Cobb was arrested and charged with second degree murder. After new evidence was discovered the second degree murder charge was dismissed and Cobb was [c]harged with first degree murder. . . . During the investigation Cobb’s phone calls from the jail have been monitored. During one conversation Cobb was heard to tell his father to get the computer out of his room and put it in his father’s room. He said there are some things on there that need to be cleaned up before anyone sees them. On at least two other occasions he made reference to his parents about never letting anyone borrow your electronic equipment. On September 16, 2014[,] the Marion County Sheriff’s Dept. served a warrant on Cobb’s residence . . . and seized the Gateway laptop computer reference[d] by James Timothy Cobb.

J.A. 40, 42. The warrant authorized the search of the Gateway laptop computer in evidence for:

Any material associated with the homicide of Paul Dean Wilson Jr. stored internally on a Gateway laptop computer serial # NXY1UAA0032251C66F1601 dark gray in color belonging to or used by James Timothy Cobb. Any and all other evidence of any other crimes.

J.A. 40.

When the executing officer began to open the computer files, he quickly discovered pornographic photos of underage females in various stages of undress and engaged in sexual acts. The officer immediately stopped the search, again consulted with the state prosecutor who concurred that the pornographic images were of prepubescent females, and sent the computer to the West Virginia State Police Digital Forensic Lab. In a follow-up interview with Cobb's parents, "[n]either one of them seemed shocked that there [were] pornographic images of underage females on their son's computer," and "[t]hey both immediately blamed [Wilson] for the images being on there." J.A. 68.<sup>1</sup>

As noted above, Cobb was initially charged with second-degree murder, but the charges were upgraded to first-degree murder due, in part, to the 911 calls and the inconsistent stories relayed to the officers by Cobb's parents. The officers later suspected that the child pornography was the motive for the murder. Months later, Cobb's cellmate told investigators that Cobb had admitted to killing Wilson because Wilson had discovered the child pornography on Cobb's computer and had threatened to turn him in to the authorities. Cobb ultimately pled guilty to second-degree murder and was sentenced to 20 years' imprisonment in state prison.

---

<sup>1</sup> According to the government, "Cobb's browsing history showed that his computer was used on at least 13 days in the month leading up to Mr. Wilson's death to search for and access child pornography, including every day of the seven days immediately preceding Mr. Wilson's death. On the dates and times that the child pornography found on Mr. Cobb's computer was downloaded, Mr. Cobb was logged in under his name and/or his known aliases on Facebook and Yahoo from the same IP address." J.A. 200-01 (footnote omitted). Cobb does not challenge these assertions on appeal.

On May 1, 2018, a federal grand jury indicted Cobb for possession of child pornography, in violation of 18 U.S.C. §§ 2252A(a)(5)(B) and (b)(2). Cobb moved to suppress the child pornography found on the computer during the murder investigation. He argued that the warrants were unsupported by probable cause as required by the Fourth Amendment to the United States Constitution. In a supplemental pleading, Cobb asserted that the second warrant was also invalid under the Fourth Amendment because it lacked the requisite particularity.

The federal magistrate judge recommended that the district court grant in part and deny in part the motion to suppress. He concluded that both warrants were supported by probable cause to believe that evidence of the murder was contained on the computer, and that the first search warrant was sufficiently particular to satisfy the Fourth Amendment. With regard to the second search warrant, he concluded that the constitutional sufficiency of the warrant was not affected by the superfluous “any and all evidence of any other crime” phrase contained at the end of the warrant, but that the motion to suppress should be granted because the balance of the second warrant was insufficiently particular to satisfy the Fourth Amendment. The magistrate judge also recommended that the district court reject the government’s request that the court apply the good-faith exception to the exclusionary rule, recognized by the Supreme Court in *United States v. Leon*, 468 U.S. 897 (1984). The government filed objections to the magistrate judge’s conclusions that the second warrant was not sufficiently particular and that the good-faith exception was inapplicable. Cobb responded, but filed no objections to the magistrate judge’s other recommendations.

The district court adopted in part and rejected in part the magistrate judge's recommendation and denied the motion to suppress. The court adopted the magistrate judge's conclusions that both warrants were supported by probable cause to believe that evidence of Wilson's murder would be found on the computer, and that "the constitutional sufficiency of both warrants was not affected by the superfluous language each contained," J.A. 239. Neither conclusion had been objected to by Cobb.

However, the district court rejected the magistrate judge's recommendation that the balance of the second warrant be found lacking in the requisite particularity. The warrant was sufficiently particular under our precedent, the district court reasoned, because it identified the specific illegal activity under investigation—the murder of Wilson on September 7, 2014. Relying on our precedent in *United States v. Williams*, 592 F.3d 511 (4th Cir. 2010), the district court also held that the child pornography was admissible under the plain-view exception to the warrant requirement. In the alternative, the district court held that the child pornography was admissible under *Leon's* good-faith exception to the suppression rule.

Cobb thereafter entered a conditional plea of guilty to the child pornography charge, reserving the right to appeal the district court's ruling on the motion to suppress. He was sentenced to 110 months in prison, to be served concurrent with the remainder of his 20-year state sentence for second-degree murder, followed by a 10-year term of supervised release.

## II.

The Fourth Amendment provides that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. Probable cause exists when, “given all the circumstances set forth in the affidavit . . . , there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Illinois v. Gates*, 462 U.S. 213, 238-39 (1983). “Unlike the probable cause requirement, which concerns the showing made by an officer *seeking* a search warrant, the particularity requirement is focused as well on the officer *executing* a warrant, and ensures that the search ‘will be carefully tailored to its justifications’ rather than becoming a ‘wide ranging exploratory search[]’ of the kind the ‘Framers intended to prohibit.’” *United States v. Blakeney*, 979 F.3d 851, 861 (4th Cir. 2020) (quoting *Maryland v. Garrison*, 480 U.S. 79, 84 (1987)).

On appeal, Cobb does not challenge the district court’s determination that both warrants were supported by probable cause to believe that evidence pertinent to the murder of Wilson would be found on Cobb’s computer. Nor does Cobb contend that the first warrant was insufficiently particular. Rather, he limits his challenge to a claim that the second warrant was not sufficiently particular because it was not “tailored to the facts presented to the police about the homicide,” and failed to explain “the types of files sought, the location of the files, the timeframe or the relationship between the files and information about the homicide.” Brief of Appellant at 11. When reviewing a district court’s denial of a motion to suppress, “we review the district court’s legal conclusions *de novo* and its

factual findings for clear error.” *United States v. Phillips*, 588 F.3d 218, 223 (4th Cir. 2009).

A.

It is well-settled that the Fourth Amendment “does not set forth some general ‘particularity requirement.’” *United States v. Grubbs*, 547 U.S. 90, 97 (2006). So long as there is probable cause to believe that “contraband or evidence of a crime will be found in a particular place,” *Gates*, 462 U.S. at 238, the Fourth Amendment “specifies only two matters that must be ‘particularly described’ in the warrant: ‘the place to be searched’ and ‘the persons or things to be seized.’” *Grubbs*, 547 U.S. at 97 (alteration omitted); *see also Blakeney*, 949 F.3d at 862.

“As always, ‘the ultimate touchstone of the Fourth Amendment is reasonableness.’” *United States v. Lyles*, 910 F.3d 787, 791 (4th Cir. 2018) (quoting *Fernandez v. California*, 571 U.S. 292, 298 (2014)). “When it comes to particularity, we construe search warrants in a ‘commonsense and realistic’ manner, avoiding a ‘hypertechnical’ reading of their terms.” *Blakeney*, 949 F.3d at 862 (quoting *Williams*, 592 F.3d at 519). “[T]he test for the necessary particularity is a pragmatic one: The degree of specificity required when describing the goods to be seized may necessarily vary according to the circumstances and type of items involved. There is a practical margin of flexibility permitted by the constitutional requirement for particularity in the description of items to be seized.” *United States v. Jacob*, 657 F.2d 49, 52 (4th Cir. 1981) (internal quotation marks and alterations omitted).

The circumstances that lead us to affirm the district court’s decision in this case are straightforward. The officers had probable cause to believe that the computer seized during the search of Cobb’s home contained evidence pertaining to Wilson’s murder—largely because Cobb, within 48 hours of the murder, instructed his parents to remove the computer from his room and clean it because Wilson had recently used it. The warrant set forth the justification for the search of the computer in some detail. In addition to setting forth facts pertaining to the murder of Wilson by Cobb, and the charges that were brought both initially and as upgraded, the warrant also referenced “Cobb’s phone calls from the jail” to his parents. J.A. 42.

During one conversation Cobb was heard to tell his father to get the computer out of his room and put it in his father’s room. *He said there are some things on there that need to be cleaned up before anyone sees them.* On at least two other occasions he made reference to his parents about never letting anyone borrow your electronic equipment.

J.A. 42 (emphasis added).

Clearly, these facts and circumstances amply provided probable cause to believe that evidence pertinent to Wilson’s murder was located on the computer and that Cobb was seeking to destroy it—a point no longer in dispute. The challenged warrant, in turn, specified as much as it reasonably could have: (1) the place to be searched—the internal contents of the “Gateway laptop computer . . . belonging to or used by James Timothy Cobb,” identified by a physical description and serial number as the one seized pursuant to the first search warrant; and (2) the things to be seized—the “material associated with the homicide of Paul Dean Wilson Jr.,” which occurred during the “domestic altercation” at their shared home on September 7, 2014. J.A. 40.

1.

We have long recognized that “[a] warrant need not—and in most cases, cannot—scrupulously list and delineate each and every item to be seized. Frequently, it is simply impossible for law enforcement officers to know in advance exactly what . . . records the defendant maintains or how the case against him will unfold.” *Phillips*, 588 F.3d at 225; *cf. United States v. Dornhofer*, 859 F.2d 1195, 1198 (4th Cir. 1988) (“[W]e do not read the search warrant as a constitutional strait jacket: that only those items particularly described in a warrant may be seized without regard to the facts and circumstances of the particular case.”) (internal quotation marks omitted).

Accordingly, “where a warrant does not *otherwise* describe the evidence to be seized, that gap can be filled, at least sometimes, if the warrant instead specifies the relevant offense.” *Blakeney*, 949 F.3d at 862-63; *see also United States v. Dickerson*, 166 F.3d 667, 693-94 (4th Cir. 1999) (upholding warrant authorizing officers to seize “[e]vidence of the crime of bank robbery”), *rev’d on other grounds, Dickerson v. United States*, 530 U.S. 428 (2000); *United States v. Jones*, 31 F.3d 1304, 1313 (4th Cir. 1994) (upholding constitutionality of warrant that “confine[d] the executing inspectors’ discretion by allowing them to seize only evidence of a particular crime”); *United States v. Fawole*, 785 F.2d 1141, 1144 (4th Cir. 1986) (warrant authorizing the broad seizure of “address books, diaries, business records, documents, receipts” was sufficiently particular because it allowed the officers “to seize only evidence of a particular crime”); *United States v. Ladd*, 704 F.2d 134, 136 (4th Cir. 1983) (upholding constitutionality of warrant that limited the officers’ seizure to “items . . . relating to ‘the smuggling, packing, distribution and use of

controlled substances”).<sup>2</sup> We hold that the district court correctly concluded that the search warrant challenged in this case was sufficiently particular because it too confined the executing officers’ discretion by allowing them to search the computer and seize evidence of a specific illegal activity—Wilson’s murder on September 7, 2014.

2.

Like the district court, we also reject Cobb’s claim that, in addition to specifying the crime under investigation, the warrant should have *also* described the “types of files sought, the location of the files, the timeframe [and] the relationship between the files and information” that the police had about Wilson’s murder. Brief of Appellant at 11. Cobb does not explain, in any meaningful way, exactly how the warrant *could* have specified the files that contained the evidence of murder. But even if it were true that the warrant *could* have been more specific, the Fourth Amendment simply did not demand that the warrant *be* more specific in this case.

The Supreme Court has “previously rejected efforts to expand the scope of [the particularity] provision to embrace unenumerated matters.” *Grubbs*, 547 U.S. at 97; *see id.* at 97-99 (rejecting challenge to the particularity of an anticipatory warrant because the warrant did not include the conditions precedent to execution of the warrant); *see also Dalia v. United States*, 441 U.S. 238, 257 (1979) (“Nothing in the language of the

---

<sup>2</sup> In like vein, a warrant need not “*always . . . specify the crime for which the executing officers may seek evidence*” *United States v. Blakeney*, 949 F.3d 851, 862 (4th Cir. 2020) (emphasis added). “Particularity with respect to the criminal activity suspected is [also] not on that list” of things that the Fourth Amendment demands. *Id.*

Constitution or in this Court’s decisions interpreting that language suggests that . . . search warrants also must include a specification of the precise manner in which they are to be executed.”). And, to the extent any question remained, this circuit recently made clear that “a warrant may satisfy the particularity requirement *either* by identifying the items to be seized by reference to a suspected criminal offense *or* by describing them in a manner that allows an executing officer to know precisely what he has been authorized to search for and seize.” *Blakeney*, 949 F.3d at 863. The warrant need not satisfy *both* criteria. *See id.*

To the extent Cobb’s challenge speaks more to the requisite specificity as to the “place” to be searched when the “place” is a computer, it also fails. In *United States v. Williams*, we addressed a similar challenge to a warrant that authorized the search of a defendant’s computer for evidence of specific crimes, during which the officers inadvertently discovered images of child pornography. In addressing the application of the plain view exception to the warrant requirement, we held that, so long as the Fourth Amendment’s basic requirements of probable cause and particularity are met, the executing officers are “impliedly authorized . . . to open each file on the computer and view its contents, at least cursorily, to determine whether the file [falls] within the scope of the warrant’s authorization—*i.e.*, whether it relate[s] to the designated . . . crimes.” *Williams*, 592 F.3d at 521-22.<sup>3</sup>

---

<sup>3</sup> Cobb’s argument that *Williams* does not apply because the ruling was based on the fact that the crimes being investigated were computer-based crimes does not avail him. Although the *Williams* court did hold that the child pornography seized was within the *scope* of the warrant, the court also held, in the alternative, that the evidence was admissible under the plain view doctrine because the officers were implicitly authorized to open, at (Continued)

Here, the warrant authorized a search of the specific computer that Cobb had asked his parents to retrieve from his bedroom, keep safe in their room, and “clean” because Cobb’s victim had recently used it. It is true that the officers suspected the computer might contain evidence explaining *why* Cobb killed Wilson, and *whether* he planned to murder him, by suffocation or by other means. And it is arguable that the evidence of child pornography *was* the evidence of motive that Cobb sought to wipe from the computer. But, as the district court correctly observed, the officers had no way of knowing when they applied for the warrant exactly *what* the evidence was that Cobb sought to destroy, or *where* Cobb had placed the evidence on the computer. The officers had probable cause to believe that Cobb’s computer contained evidence pertinent to Cobb’s murder of Wilson on September 7, 2014, and that Cobb’s parents were willing to lie, destroy evidence, and manufacture evidence to support the narrative that Cobb’s murder of Wilson was defensive in nature. Accordingly, more specificity was not required under the Fourth Amendment, nor was limiting the scope of the computer search practical or prudent under the circumstances of this investigation.

In sum, even if the Fourth Amendment might require more specificity as to the place to be searched or the items to be seized in some computer searches, Cobb has failed to convince us that the Fourth Amendment demanded that the descriptions of the place to be searched and the things to be seized needed to be more specific in this case. At bottom, his argument boils down to the claim that, even though probable cause existed to believe that

---

least briefly, the computer files to locate the evidence of the specific crime referenced in the warrant.

incriminating evidence pertaining to the murder of Wilson was located on that computer, and that Cobb was seeking to destroy it, the police could not search the computer because the police could not *foretell* the murder evidence that was located on the computer or the location of that evidence within the contents of the computer. That is not what the Fourth Amendment demands.

B.

We also affirm the district court’s ruling that the constitutionality of the warrant was unaffected by the superfluous language included at the end of the warrant. Although we agree that the phrase “[a]ny and all evidence of any other crimes,” standing alone, is overbroad, it did not render the entire warrant invalid.

Under the severance doctrine, “the constitutionally infirm portion” of a warrant—“usually for lack of particularity or probable cause—is separated from the remainder and evidence seized pursuant to that portion is suppressed; evidence seized under the valid portion may be admitted.” *United States v. George*, 975 F.2d 72, 79 (2d Cir. 1992). “This notion that a search conducted pursuant to a warrant held unconstitutional in part does not invalidate the entire search is signaled in cases stating that only those items seized beyond the warrant’s scope must be suppressed.” *Id.* “[T]he social gains of deterring unconstitutional police conduct by suppressing *all* evidence seized pursuant to a partially invalid warrant often are outweighed by the social costs occasioned by such an across the board ruling.” *Id.*; *see also United States v. Sells*, 463 F.3d 1148, 1154-55 (10th Cir. 2006) (“In accordance with the purposes underlying the warrant requirement and the exclusionary rule, every federal court to consider the issue has adopted the doctrine of severance,

whereby valid portions of a warrant are severed from the invalid portions and only material seized under the authority of the valid portions, or lawfully seized while executing the valid portions, are admissible.”) (footnotes omitted).

Although this court has not yet referred to the “severance doctrine” by name in a published opinion, we have applied it in similar circumstances. In *United States v. Jacob*, we agreed that “the general tail of [a] search warrant,” which seemingly authorized a search for violations of *any* federal criminal law, did not defeat the otherwise sufficiently-particular portion of the warrant. *Jacob*, 657 F.2d at 51-52. “[C]onsistent with the standard of our circuit which seeks to avoid the suppression of evidence seized pursuant to a warrant because of ‘hypertechnical’ errors,” we held that “a defective qualifying phrase will not defeat a warrant which is otherwise sufficiently specific.” *Id.* at 52. Rather, “the challenged phrase should properly be treated as merely superfluous and falls within the ‘practical margin of flexibility’ afforded warrants in cases of this type.” *Id.*

Since then, at least two panels of this court have recognized this severance doctrine in unpublished cases. In *United States v. Prince*, for example, we declined to invalidate a warrant which contained “broad boilerplate language authorizing seizure of every conceivable item without tying these items to the alleged crimes or circumstances of the case.” 187 F.3d 632, 1999 WL 511003, at \*6 (4th Cir. 1999).

We have held that, in order to avoid the suppression of lawfully seized evidence, a warrant that properly identifies some items “will not be defeated by other ambiguous or conclusionary language” so long as the warrant was “sufficiently particularized with respect to the items seized.” *United States v. Jacob*, 657 F.2d 49, 52 (4th Cir. 1981). In other words a court will “sever” the too general portion of the warrant from the sufficiently specific portion. *See United States v. George*, 975 72, 79 (2d Cir. 1992).

*Id.* In such cases, “[t]he evidence obtained pursuant to the lawful portion of the warrant [is] rightly admitted [and] the remainder of the warrant, while too broad, provides no basis for reversal.” *Id.* at \*7.

And in *United States v. Walker*, 403 F. Appx. 803, 805-06 (4th Cir. 2010), we held that, although the warrant at issue improperly authorized the seizure of items (controlled substances) that was not supported by probable cause, the offending phrase would be redacted and the balance of the warrant upheld.

[A]bsent a showing of pretext or bad faith on the part of the police or the Government, the invalidity of part of a search warrant does not require the suppression of all the evidence seized during its execution. *See United States v. Fitzgerald*, 724 F.2d 633, 636-37 (8th Cir. 1983). Thus, even if the portion of the warrant permitting seizure of [controlled substances] is invalid, the Fourth Amendment does not require the suppression of anything described in the valid portions of the warrant or “lawfully seized [] on plain-view grounds, for example—during their execution.” *Id.* at 637; *see also United States v. George*, 975 F.2d 72, 79 (2d Cir. 1992) (holding that, where warrant as a whole is not invalid, a redacted warrant may justify a police intrusion, permitting admission of items found in plain view).

*Id.* at 806.

We agree with these applications of the severance doctrine, and hold that the challenged phrase “[a]ny and all evidence of any other crimes” in the warrant before us, while overbroad in isolation, was easily and properly severed from the balance of the warrant which, as we have explained, was sufficiently particularized. Rather than invalidate the entire warrant and require suppression of the evidence of child pornography found in plain view on the computer, “the challenged phrase [was] properly . . . treated as merely superfluous and falls within the ‘practical margin of flexibility’ afforded warrants in cases of this type.” *Jacob*, 657 F.2d at 52.

Perhaps because this point is so well established, we also note that Cobb failed to properly preserve appellate review of it. The magistrate judge noted in his report and recommendation our holdings that such “generalizing” or “catch-all” phrases will not ordinarily invalidate an otherwise sufficiently particular warrant, J.A. 186, and ruled only that the first part of the warrant was *not* sufficiently particular. And because “[n]either party objected to [the magistrate judge’s] conclusion that the constitutionality of [the] warrants was unaffected by the superfluous language included in [them],” the district court adopted the finding and ruled accordingly. J.A. 250. Cobb, therefore, failed to preserve appellate review of the substance of the magistrate judge’s recommendation. *See Martin v. Duffy*, 858 F.3d 239, 245 (4th Cir. 2017) (“A plaintiff is deemed to have waived an objection to a magistrate judge’s report if he does not present his claims to the district court.”) (internal quotation marks and alterations omitted). Moreover, although Cobb obliquely asserts in his opening brief that the catch-all phrase in the second warrant made the first part of the warrant “worse,” Appellant’s Brief at 11-12, he did not directly challenge the district court’s ruling on the effect of the superfluous language, nor did he brief the issue in his opening brief to this court. *See Muth v. United States*, 1 F.3d 246, 250 (4th Cir. 1993) (“As this court has repeatedly held, issues raised for the first time on appeal generally will not be considered.”); *see also Cavallo v. Star Enter.*, 100 F.3d 1150, 1152 n.2 (4th Cir. 1996) (“[A]n issue first argued in a reply brief is not properly before a court of appeals.”).

C.

We also affirm the district court’s application of the plain view doctrine to the evidence of child pornography. “Once it is accepted that a computer search must, by implication, authorize at least a cursory review of each file on the computer, then the criteria for applying the plain-view exception are readily satisfied.” *Williams*, 592 F.3d at 522. The officer “has a lawful right of access to all files, albeit only momentary,” and “when the officer then comes upon child pornography, it becomes immediately apparent that its possession by the computer’s owner is illegal and incriminating.” *Id.* (internal quotation marks and citations omitted).

Cobb’s sole challenge to the district court’s application of the plain view exception is based upon his argument that the warrant was not sufficiently particular and, therefore, that the officers could not have been lawfully present at the place where the child pornography was plainly viewed. In light of our ruling on the particularity of the warrant, we affirm the district court’s determination that the child pornography was admissible under the plain view doctrine.

#### D.

Finally, we reject Cobb’s belated request, supported by the ACLU’s amicus brief, that we not follow our prior holding in *United States v. Williams*, and hold instead that ordinary principles of Fourth Amendment jurisprudence, including the plain view doctrine, should not apply to computer searches. In *Williams*, we rejected the defendant’s nearly identical claim that “traditional Fourth Amendment rules cannot be successfully applied in th[e] context” of computer searches because computers “hold so much information, touching on virtually every aspect of a person’s life,” and that “a new approach is needed

for applying the Fourth Amendment to searches of computers and digital media.” 592 F.3d at 517.

Even if Cobb had raised such a direct challenge below or in his opening brief, we are powerless to overrule the decision of a prior panel of this court. *See McMellon v. United States*, 387 F.3d 329, 332 (4th Cir. 2004) (en banc) (explaining the “basic principle that one panel cannot overrule a decision issued by another panel”). Nor would we reject *Williams*’ application to the warrant in this case. As we have explained above, “[n]othing in the language of the Constitution or in [the Supreme] Court’s decisions interpreting that language suggests that, in addition to the requirements set forth in the text, search warrants also must include a specification of the precise manner in which they are to be executed.” *Dalia*, 441 U.S. at 257. “On the contrary, it is generally left to the discretion of the executing officers to determine the details of how best to proceed with the performance of a search warrant—subject of course to the general Fourth Amendment protection ‘against *unreasonable* searches and seizures.’” *Id.* (footnote omitted, emphasis added); *see also Dickerson*, 166 F.3d at 694 (“[T]he law of this Circuit . . . allow[s] some discretion to the officers executing a search warrant, so long as the warrant at least minimally ‘confines the executing officers’ discretion by allowing them to seize only evidence of a particular crime.’” (quoting *Fawole*, 785 F.2d at 1144)). Reasonableness in the description of the place to be searched and the things to be seized is all that the Fourth Amendment demands,

and the warrant to search this computer, based upon the circumstances and the type of evidence sought in this case, was sufficiently particular in both respects.<sup>4</sup>

III.

For the foregoing reasons, we affirm the judgment of the district court.

AFFIRMED

---

<sup>4</sup> In light of our holding, we need not address the district court's alternative ruling that the *Leon* good faith exception applies. See *United States v. Leon*, 468 U.S. 897 (1984).

FLOYD, Circuit Judge, dissenting:

I disagree with my colleagues in the majority as to the constitutionality of the search warrant that authorized the search of the laptop. For the reasons explained herein, I would hold that the search warrant was unconstitutional for lack of particularity as to the items to be seized, that the government cannot rely on the plain-view exception for the seizure of the child pornography found on the laptop, and that the good-faith exception to the exclusionary rule does not apply. As a result, I would hold that the district court erred and that the child pornography should be suppressed.

I.

A.

In September 2014, James Cobb was living with his parents, James Keith Cobb (Cobb Sr.) and Freda Cobb (Ms. Cobb), near Fairmont, West Virginia. Cobb's cousin, Paul Dean Wilson, also lived at the home.

On September 7, 2014, a feud occurred between Cobb and Wilson. By the end of this family feud, Cobb had suffocated Wilson to death. During a 911 call made at the time of the altercation, Ms. Cobb was heard telling her son: "he's helpless" and "you[re] going to end up killing the man." J.A. 54. Cobb was subsequently charged with second-degree murder.<sup>1</sup>

---

<sup>1</sup> The charge was later upgraded to first-degree murder. However, as discussed below, Cobb eventually pleaded guilty to second-degree murder.

In the course of the murder investigation, three conflicting stories emerged as to what started the altercation between Cobb and Wilson. Cobb told investigators that the fight started because Wilson's firearm was not in the place where he had left it. However, Cobb's parents gave different accounts. Cobb Sr. told investigators that the fight started because Wilson was threatening Cobb Sr. and Cobb stepped in. By contrast, Ms. Cobb claimed that the fight started because Wilson was mean to his cat and, when Ms. Cobb told Wilson to stop, Wilson punched her in the mouth, prompting Cobb to step in.<sup>2</sup>

A couple of days after the killing, on September 9, 2014, Cobb told Cobb Sr. in a recorded jail call to get his laptop out of Cobb's bedroom and put it in his room "to keep it safe," and that he should "clean" it. J.A. 163. In this phone call, Cobb stated that Wilson borrowed the laptop and that he had put some "shit" on it. J.A. 163.

On September 16, 2014, after listening to the recorded jail phone call, the police sought and obtained a search warrant for the home (the "first search warrant"). The search warrant stated that the following list of items were to be seized:

Any and all firearms belonging to Paul Dean Wilson Jr., any and all laptop computers, including tablets or desktop computers belonging to or operated by James Timothy Cobb, any and all cellphones belonging to or operated by James Timothy Cobb, and any and all evidence of a crime.

J.A. 36.

---

<sup>2</sup> Notably, Ms. Cobb's account of the events was brought into question in a recorded jail telephone call. Ms. Cobb told Cobb that a neighbor had told her to put cotton in her lip and take a picture, and that she had heeded the advice and provided the picture to police.

On the same day, the police executed the first search warrant, seizing a Gateway laptop (the “laptop”), among other items.

On September 23, 2014, the police requested and were granted another search warrant to search the contents of the laptop (the “second search warrant”). The second search warrant authorized a search for:

Any material associated with the homicide of Paul Dean Wilson Jr. stored internally on a Gateway laptop computer serial #NXY1UAA0032251C66F1601 dark gray in color belonging to or used by James Timothy Cobb. Any and all evidence of any other crimes.

J.A. 40. The probable cause statement in the second search warrant was as follows:

On September 7, 2014[,] the Marion County Sheriff’s Dept. responded to a domestic altercation between James Timothy Cobb and Paul Dean Wilson Jr.[] who are cousins both living with Cobb’s parents . . . in Marion Co. Wilson was pronounced dead at the scene. Cobb was arrested and charged with second degree murder. After new evidence was discovered the second degree murder charge was dismissed and Cobb was [c]harged with first degree murder. . . . During the investigation Cobb’s phone calls from the jail have been monitored. During one conversation Cobb was heard to tell his father to get the computer out of his room and put it in his father’s room. He said there are some things on there that need to be cleaned up before anyone sees them. On at least two other occasions he made reference to his parents about never letting anyone borrow your electronic equipment. On September 16, 2014[,] the Marion County Sheriff’s Dept. served a search warrant on Cobb’s residence . . . and seized the Gateway laptop computer referenced by James Timothy Cobb.

J.A. 40, 42.

When the executing officer, Sgt. Alkire, executed the second search warrant and began opening computer files, he stumbled upon photos of prepubescent girls.

On August 29, 2017, Cobb entered a plea of guilty to second-degree murder in state court in Marion County, West Virginia. He was sentenced to 20 years in state prison.

On May 1, 2018, a federal jury in the Northern District of West Virginia returned an indictment charging Cobb with possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B), (b)(2). On June 15, 2018, Mr. Cobb entered a plea of not guilty.

B.

On July 6, 2018, Cobb moved to suppress the evidence seized per the first and second search warrants. Relevant for purposes of this appeal, Cobb argued that the second search warrant allowing a search of the contents of the laptop was unconstitutionally broad in scope and “entirely lack[ed] particularity of the information or electronic files to be seized[,] . . . leav[ing] all of Mr. Cobb’s personal information contained in the laptop at the unfettered discretion of the State.” J.A. 94.

On July 19 and 23, 2018, a suppression hearing was held before a federal magistrate judge. The government called no witnesses. Cobb called two witnesses to testify: Sgt. Alkire, the attesting officer to the second search warrant, and Magistrate Cathy Reed-Vanata, the state magistrate who issued the second search warrant.

Sgt. Alkire described his role in the investigation, including that he assisted in executing the first search warrant and drafted and obtained the second search warrant. According to his testimony, Sgt. Alkire had previously applied for search warrants involving computers, including the internal contents of a computer, and that he drafted the second search warrant in the same manner that he had drafted such warrants in the past. Sgt. Alkire testified that he used the language “[a]ny and all evidence of any other crime” in nearly every search warrant that he had drafted because that was the way he had been taught to draft warrants. J.A. 114.

In obtaining the second search warrant, Sgt. Alkire testified that, although he did not show the county prosecutor, Pat Wilson, a copy of the warrant, he did confer with him in getting the warrant. Sgt. Alkire testified that the magistrate judge did not question the “any and all evidence of other crimes” language, and that in the approximately 100 search warrants that Sgt. Alkire had obtained with such language, no one had ever told him that he should not include the phrase. In fact, Sgt. Alkire testified that it was “pretty much standard practice for us. We — we do that on about every one and we’ve never been told otherwise.” J.A. 146.

Having obtained the second search warrant, Sgt. Alkire returned to his office and, despite never searching a computer before, conducted the search of the laptop. He testified that he was mainly looking for “[p]hotographs and files” relating to suffocation or any other evidence that might shine light on the motive for the killing. J.A. 126. According to Sgt. Alkire, it did not “take very long” to find child pornography. J.A. 125. After he found a few photos of prepubescent girls in various stages of undress and engaged in sexual acts, he sent the laptop to the lab for further forensic analysis.

Magistrate Reed-Vanata testified she was not provided any other information regarding the investigation not contained in the four corners of the affidavit and that she did not ask any questions as that was not the “appropriate practice.” J.A. 166. She also testified that the phrase “any and all evidence” was not new to her and had been proposed to her before in search warrants that she had granted. J.A. 166.

On August 24, 2018, the federal magistrate judge issued a report and recommendation concluding that the second search warrant lacked sufficient particularity

because it did not identify the items to be seized from the laptop. Further, the magistrate judge held that the *Leon* good-faith exception to the exclusionary rule did not apply and so the child pornography should be suppressed. See *United States v. Leon*, 468 U.S. 897, 923 (1984).

On November 10, 2018, the district court issued its decision adopting in part and rejecting in part the magistrate judge's report and recommendation. The district court held that the second search warrant was sufficiently particular. *United States v. Cobb*, No. 1:18CR33, 2018 WL 4907764, at \*5 (N.D. W. Va. Oct. 10, 2018). Moreover, the district court held that even if the second search warrant was not sufficiently particular, the evidence would be admissible under the plain-view exception. *Id.* Further still, the district court held that even if the search violated the Fourth Amendment, the *Leon* good-faith exception to the exclusionary rule applied. *Id.* at \*5–6. As a result, the district court denied Cobb's motion to suppress. *Id.* at \*7.

Thereafter, on October 12, 2018, Cobb entered a conditional guilty plea to possessing child pornography, reserving his right to appeal the denial of his motion to suppress. Cobb was sentenced to 110 months of imprisonment (to be served concurrently with his state murder conviction) and 10 years of supervised release. This appeal followed.

## II.

On appeal, Cobb raises three main issues. First, he contends that the second search warrant was unconstitutional for lack of particularity. Second, he contends that the plain-view exception to the Fourth Amendment's warrant requirement is inapplicable. Finally,

he argues that the government cannot rely on the *Leon* good-faith exception to the exclusionary rule.

This Court reviews factual findings in a suppression motion for clear error and the legal conclusions de novo. *United States v. Pratt*, 915 F.3d 266, 271 (4th Cir. 2019).

A.

First, I turn to the issue of whether the district court erred in holding that the second search warrant was sufficiently particular. On appeal, Cobb argues that the second search warrant violated the Fourth Amendment’s particularity requirement as it did not specify the types of evidence investigators were looking for on the laptop beyond evidence “associated with the homicide of [Wilson].” J.A. 40.

Under the Fourth Amendment, a warrant must “particularly describe[e] the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. This is referred to as the “particularity requirement.” The Fourth Amendment and its particularity requirement sprung from colonial opposition to “indiscriminate searches and seizures conducted under the authority of ‘general warrants’” known as writs of assistance. *Payton v. New York*, 445 U.S. 573, 583 (1980). Such writs of assistance gave customs officials “broad latitude to search houses, shops, cellars, warehouses, and other places for smuggled goods” imported in violation of British tax laws. *United States v. Wurie*, 728 F.3d 1, 3 (1st Cir. 2013); see *Stanford v. Texas*, 379 U.S. 476, 481 (1965). In a 1761 case challenging the use of such writs in Massachusetts, James Otis famously decried that writs of assistance were the “worst instrument of arbitrary power,” as they placed “the liberty of every man in the hands of every petty officer.” *Stanford*, 379 U.S. at 481.

The opposition to the use of writs of assistance was not a novel pushback against perceived government overreach. In fact, the struggle in the early years of this Nation against the use of writs of assistance was preceded by an “earlier . . . struggle against oppression which had endured for centuries” in England. *Id.* at 482. During the sixteenth, seventeenth, and eighteenth centuries, the Crown used general warrants in enforcing literature licensing and, later, in prosecuting seditious libel. *Id.* Such general warrants “typically authorized of all persons connected of the premises of all persons connected with the publication of a particular libel, or the arrest and seizure of all the papers of a named person thought to be connected with a libel.” *Id.* at 482–83.

The resistance to such Government intrusion culminated in landmark English cases such as *Entick v. Carrington*. 19 How. St. Tr. 1029 (1765). John Entick was the author of a publication titled *Monitor or British Freeholder*. *Stanford*, 379 U.S. at 483. A warrant was issued naming him and his publication and authorizing his arrest for seditious libel and seizure of his “books and papers.” *Id.* In executing the warrant, over the course of four hours the King’s Messengers ransacked Entick’s house, breaking open doors, locks, boxes, chests, and drawers; reading all of Entick’s private papers and books; and carrying away many of Entick’s papers. In the famous case, Lord Camden declared the warrant to be unlawful. “This power,” Lord Camden stated, “so assumed by the secretary of state is an execution upon all the party’s papers, in the first instance.” *Id.* at 484 (citing *Entick*, 19 How. St. Tr. at 1064). “His house is rifled; his most valuable secrets are taken out of his possession, before the paper for which he is charged is found to be criminal by any competent jurisdiction, and before he is convicted either of writing, publishing, or being

concerned in the paper.” *Id.* (quoting *Entick*, 19 How. St. Tr. at 1064). After this case, the House of Commons “passed two resolutions condemning general warrants, the first limiting its condemnation to their use in cases of libel, and the second condemning their use generally.” *Id.* The case of *Entick v Carrington* has been described by our Supreme Court as the “wellspring of the rights now protected by the Fourth Amendment.” *Id.*

Considering this history, the Supreme Court has stated that the purpose of the particularity requirement is to make general searches “impossible.” *Marron v. United States*, 275 U.S. 192, 196 (1927). A sufficiently particular warrant therefore avoids “a general, exploratory rummaging in a person’s belongings.” *Andresen v. Maryland*, 427 U.S. 463, 480 (1976); *see also United States v. Dargan*, 738 F.3d 643, 647 (4th Cir. 2013) (stating that the particularity requirement precludes “officers from conducting fishing expeditions into the private affairs of others”). As this Court has stated: “The particularity requirement is fulfilled when the warrant identifies the items to be seized by their relation to designated crimes and when the description of the items leaves nothing to the discretion of the officer executing the warrant.” *United States v. Williams*, 592 F.3d 511, 519 (4th Cir. 2010).

Here, the second search warrant authorized a search for “[a]ny material associated with the homicide of [Wilson] stored internally on [the laptop] . . . . Any and all evidence of other crimes.” J.A. 40. The question is whether the limiting language that the material had to be “associated with the homicide” of Wilson made the warrant sufficiently particular. For the reasons explained below, I conclude that it did not.

The particularity requirement of the Fourth Amendment is “a pragmatic one: The degree of specificity required when describing the goods to be seized may necessarily vary according to the circumstances and type of items involved.” *United States v. Dickerson*, 166 F.3d 667 (4th Cir. 1999), *rev’d in part on other grounds*, 530 U.S. 428 (2000); *see also United States v. Yusuf*, 461 F.3d 374, 395 (3d Cir. 2006) (“[T]he breadth of items to be searched depends upon . . . the information available to the investigating agent that could limit the search at the time the warrant application is given to the magistrate.”); *United States v. Spilotro*, 800 F.2d 959, 963 (9th Cir. 1986) (“The specificity required in a warrant varies depending on the circumstances of the case and the type of items involved. Warrants which describe generic categories of items are not necessarily invalid if a more precise description of the items subject to seizure is not possible.”).

Here, at the time the second search warrant was issued, there were three different explanations for what prompted the altercation between Cobb and Wilson—namely, Wilson being unable to find his firearm, Cobb stepping in to protect Cobb Sr., and Wilson being mean to his cat and punching Ms. Cobb when she stepped in. Adding a possible fourth explanation to the mix, Sgt. Alkire knew, based on Cobb’s recorded jail calls, that Wilson may have downloaded something on the laptop in the days before the altercation. At the suppression hearing, Sgt. Alkire testified that he was looking for evidence of motive that could help justify the first-degree murder charge and that he wanted to look at photographs, files, and searches about suffocations. As the federal magistrate judge concluded rightly: “All of this information could have been used to limit the search. The search warrant could have been limited to the files that were testified to by Sgt. Alkire at

[the] suppression hearing—internet searches about suffocations and files—with the addition of a time limit—that have been accessed and/or added within the previous two weeks (or some time limit).” J.A. 180. Although the authorities had some suggestions as to possible motives, they failed to cabin the search warrant to the facts known at the time. Instead, the second search warrant lacked any particularity beyond information “associated with the homicide” of Wilson. Sgt. Alkire could have limited—and, in my view, was constitutionally required to limit—the search based on the information known to authorities at the time. *United States v. Fuccillo*, 808 F.2d 173, 176 (1st Cir. 1987) (“In light of the information available to the agents which could have served to narrow the scope of the warrant and protect the defendants’ personal rights, the warrant was inadequate.” (quoting *United States v. Klein*, 565 F.2d 183, 190 (1st Cir. 1977))).

It is true that this Court has recognized that, where a warrant does not sufficiently describe the evidence to be seized, the particularity “gap can be filled, at least *sometimes*, if the warrant instead specifies the relevant offense.” *United States v. Blakeney*, 949 F.3d 851, 862–63 (4th Cir. 2020) (emphasis added); *see also id.* (“[A] warrant may satisfy the particularity requirement *either* by identifying the items to be seized by reference to a suspected criminal offense *or* by describing them in a manner that allows an executing officer to know precisely what he has been authorized to search for and seize.”). However, the government and the majority’s reliance on this line of cases is misplaced. *See* Maj. Op. 12–13; Gov’t Br. 11–16. A warrant merely specifying the relevant offense only satisfies the particularity requirement when “a more precise description [is] not possible in the circumstances” *and* where the crime listed generates “quite distinctive evidence.”

*Dickerson*, 166 F.3d at 674 (first quoting *United States v. George*, 975 F.2d 72, 76 (2d Cir. 1992)). Neither of those preconditions are close to being satisfied here.

First, as discussed above, the government had information as to potential motives for the murder. In fact, Sgt. Alkire testified that he knew the general contours of the information he was seeking, namely, photographs, files, and searches about suffocations. Such information could have, and should have, been included in the warrant to provide a more “precise definition” of the evidence sought to be seized. *Id.* By way of example, the warrant could have authorized the search of recently downloaded files, recent search history, or communications between Wilson and Cobb.

Secondly, this is not a case in which the crime specified, the “homicide of [Wilson],” would allude to distinctive evidence. This is because there are no typical “tools of the trade” for murder, especially when the evidence sought is on a personal computer, which stores gigabytes of data, including documents, pictures, emails, videos, search history, instant messages, and the like.

*Dickerson* provides the best contrast with this case. In *Dickerson*, this Court held that a warrant for the search of a residence was sufficiently particular when it stated that the evidence to be seized was “evidence of the crime of bank robbery.” 166 F.3d at 694. In doing so, we recognized that warrants identifying the items to be seized as “evidence of [a] [specific crime]” are sometimes upheld as constitutional “where a more precise description was not possible in the circumstances.” *Id.* at 693 (second alteration in original) (citing *George*, 975 F.3d at 76). However, we explained that a warrant authorizing a search for evidence relating to “‘a broad criminal statute or general criminal activity’ such as ‘wire

fraud,’ ‘fraud,’ ‘conspiracy,’ or ‘tax evasion,’ is overbroad because it ‘provides no readily ascertainable guidelines for the executing officers as to what items to seize.’” *Id.* at 694 (quoting *George*, 975 F.3d at 76). A warrant authorizing a search for evidence relating to a “specific illegal activity” such as “narcotics” or “theft of fur coats,” by contrast, was “sufficiently particular.” *Id.* Because we held that the specific crime of bank robbery was “specific illegal activity that . . . generates quite distinctive evidence,” such as guns, masks, bait money, dye-stained bills and clothes, and carrying bags, we held the warrant in *Dickerson* adequately distinguished “between those items which are to be seized and those which are not.” *Id.*

In this case, unlike search warrants pertaining to crimes involving narcotics, the “theft of fur coats,” or bank robbery, the mere reference to first-degree murder when applied to a laptop does not readily make the evidence that is the subject of the warrant “reasonably subject to identification.” *Id.* As a result, this is not a case where the particularity requirement is satisfied by merely referencing the charged offense.<sup>3</sup>

---

<sup>3</sup> Unlike the majority, I do not address our decision in *Williams* in the context of the particularity analysis. *See* Maj. Op. 14–15. In *Williams*, the search warrant specified that the following items were to be seized: “Any and all computer systems and digital storage media, videotapes, videotape recorders, documents, photographs, and Instrumentalities indicat[ive] of the offense of [harassment by computer in violation of Va. Code Ann. §18.2-152.7:1].” 592 F.3d at 515–16 (first alteration in original). In executing the warrant, officials found a DVD containing child pornography. *Id.* at 516. *Williams* moved to suppress the DVD, arguing that the warrant did not “authorize[] officers to view each file on the computer, but rather . . . authorized a search of *only those files* in his computer related to the designated state offenses.” *Id.* at 518–19. In assessing whether the authorities exceeded the scope of the search warrant—a legal question distinct from whether a warrant is sufficiently particular—this Court held that the seizure of the child pornography was within the scope of the warrant. *Id.* at 520–21. In the alternative, the (Continued)

In summary, in the course of their investigation the authorities had gathered enough information to provide a more precise definition of the evidence sought. The officers were required to use this information to limit the breadth of the search warrant. By failing to do so, they failed to cabin the search warrant to the facts known at the time. Instead, the warrant, as drafted, provided a general warrant to rifle through the entire contents of the laptop and failed to adequately distinguish “between those items which are to be seized and those which are not.” *Id.* To countenance the current warrant would be to permit ill-defined fishing expeditions into the vast oceans of personal information stored on citizens’ digital devices. For the above reasons, the second search warrant was facially unconstitutional for lack of particularity as to the items to be seized.<sup>4</sup>

B.

Even though the second search warrant was unconstitutional, I next consider whether the district court erred in holding that the child pornography evidence is

---

Court held under the plain-view exception, discussed below, that the officers had the authority to “open each file on the computer and view its contents, at least cursorily, to determine whether the file fell within the scope of the warrant’s authorization.” *Id.* at 521. Even though this Court’s decision in *Williams* gives law enforcement broad latitude under the plain-view exception to search the contents of a computer, it does not absolve them of their responsibility to obtain a warrant that satisfies the Fourth Amendment’s particularity requirement.

<sup>4</sup> Given that I hold the operative parts of the warrant are invalid, unlike my colleagues, I do not reach the additional question of whether the superfluous phrase “[a]ny and all evidence of any other crimes” can be severed from the rest of the warrant. *See* Maj. Op. 16–19. Excising such a phrase would not save the warrant.

nevertheless admissible under the plain-view exception. For the reasons explained below, I conclude that the plain-view exception is inapplicable.

As a general rule, warrantless searches or seizures are per se unconstitutional. *Williams*, 592 F.3d at 521. However, the Supreme Court has recognized “a few specifically established and well-delineated exceptions.” *Mincey v. Arizona*, 437 U.S. 385, 390 (1978) (quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)). One such exception is that “under certain circumstances the police may seize evidence in plain view without a warrant.” *Coolidge v. New Hampshire*, 403 U.S. 443, 465 (1971) (plurality opinion). Under the plain-view exception, police may seize evidence during a lawful search if: “(1) the seizing officer is lawfully present at the place from which the evidence can be plainly viewed; (2) the seizing officer has a lawful right of access to the object itself; and (3) the object’s incriminating character [is] . . . immediately apparent.” *Williams*, 592 F.3d at 521 (alteration in original) (quotation marks omitted). The exception is grounded in the rationale that when “police are lawfully in a position to observe an item first-hand, its owner’s privacy interest in that item is lost.” *Illinois v. Andreas*, 463 U.S. 765, 771 (1983).

Here, the analysis begins and ends at first element. Although the first search warrant gave officers the lawful ability to seize the laptop, it did not give them the authority to search the laptop. That authority was purportedly conferred by the second search warrant, which, as discussed above, was facially unconstitutional. As a result, the officers did not have the lawful authority to search the laptop from which the alleged plain view occurred. In other words, when Sgt. Alkire was searching the laptop, he was not “lawfully present at

the place from which” the child pornography was viewed. *Williams*, 592 F.3d at 521. Therefore, the evidence is not admissible under the plain-view exception.

### C.

Lastly, I turn to the question of whether the evidence is nonetheless admissible pursuant to the *Leon* good-faith exception to the exclusionary rule.

The suppression of evidence obtained in violation of the Fourth Amendment (called the “exclusionary rule”) is not a remedy found in the Constitution but rather a “judicially created prescription for . . . a violation.” *United States v. Seerden*, 916 F.3d 360, 366 (4th Cir. 2019); *see United States v. Calandra*, 414 U.S. 338, 347 (1974) (holding that the exclusionary rule provides that “evidence obtained in violation of the Fourth Amendment cannot be used in a criminal proceeding against the victim of the illegal search and seizure”). The exclusionary rule is “primarily proscriptive” in that it is “designed to safeguard Fourth Amendment rights through its deterrent effect.” *Seerden*, 916 F.3d at 366. For that reason, “evidence should be suppressed ‘only if it can be said that the law enforcement officer had knowledge, or may properly be charged with knowledge, that the search was unconstitutional under the Fourth Amendment.’” *Illinois v. Krull*, 480 U.S. 340, 348–49 (1987) (quoting *United States v. Peltier*, 422 U.S. 531, 542 (1975)).

In *Leon*, the Supreme Court recognized a good-faith exception to the exclusionary rule, “under which evidence obtained by an officer who acts in objectively reasonable reliance on a search warrant will not be suppressed, even if the warrant is later deemed invalid.” *United States v. Thomas*, 908 F.3d 68, 72 (4th Cir. 2018) (citing *Leon*, 468 U.S. at 922). Importantly, however, in *Leon* Court delineated several situations in which the

good-faith exception would *not* apply, including where, “depending on the circumstances of the particular case, [the warrant is] so facially deficient—i.e., in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid.” 668 U.S. at 923. Here, Cobb argues that the warrant was so facially deficient that no reasonable officer could presume it to be valid.

As discussed above, the second search warrant was facially overbroad in that it allowed for the search for “[a]ny material associated with the homicide of [Wilson]” on the laptop. The second search warrant failed to specify the categories of information sought on the laptop; instead, it merely referred to the homicide and did not adequately distinguish *ex ante* “between those items which are to be seized and those which are not.” *Dickerson*, 166 F.3d at 693.

The fact that the second search warrant was facially deficient, however, is not the end of the good-faith inquiry. We must look to the circumstances of the case, as evidenced by *Leon*’s companion case, *Massachusetts v. Sheppard*. 468 U.S. 981, 987 (1984); *see also Dickerson*, 166 F.3d at 694 (stating that the inquiry depends “upon the understanding of a reasonable officer in light of the totality of the circumstances”). *Sheppard* involved a facially deficient warrant. But rather than categorically excluding the evidence, the Supreme Court examined the totality of the circumstances, including the officer’s knowledge and actions as well as the officer’s reliance on the statements of a district attorney and the judge who issued the warrant. 468 U.S. at 989. Although *Sheppard* involved a murder investigation, the officer used a form search warrant stating that controlled substances were the object of the search. The officer raised the issue with the

judge, and the judge assured the officer that he would make the necessary corrections to the warrant and that the warrant was valid. *Id.* at 995–96. Yet the judge failed to correct the warrant, and the officer failed to notice the error before executing the search. In holding that the evidence should not be suppressed for lack of particularity, the Supreme Court held that the officers had taken “every step that could reasonably be expected of them,” *id.* at 989, and stated that it was “the judge, not the police officers, who made the critical mistake,” *id.* at 990.

The Supreme Court again dealt with the *Leon* good-faith exception as it applies to facially deficient warrants in the case of *Groh v. Ramirez*, 540 U.S. 551, 563 (2004). There, the Supreme Court affirmed the denial of summary judgment in a 42 U.S.C. § 1983 action to an officer who sought to rely on a search warrant in which he failed to particularize the items sought. The warrant in *Groh* merely described the respondent’s two-story house, rather than the items—firearms—sought to be seized. *Id.* at 554. Contrasting the case with *Sheppard*, the Supreme Court in *Groh* stated that “because petitioner himself prepared the invalid warrant, he may not argue that he reasonably relied on the Magistrate’s assurance that the warrant contained an adequate description of the things to be seized and was therefore valid.” *Id.* at 564. Ultimately, the Supreme Court held that the officer did not have qualified immunity because the warrant was so facially deficient. *Id.* at 565.

Turning to the circumstances of this case, unlike in *Sheppard*, there is nothing in the record that suggests Sgt. Alkire received express affirmation from the magistrate that the warrant was valid (other than, of course, her signature). Additionally, like in *Groh*, Sgt. Alkire prepared the warrant himself, without assistance from the magistrate, like in

*Sheppard*. To be sure, Sgt. Alkire consulted with the local county prosecutor, Pat Wilson, about the warrant. *See United States v. Clutchette*, 24 F.3d 577, 581–82 (4th Cir. 1994) (consultation with government attorney is relevant to a finding of good faith). But that fact does not weigh against suppression, as the government claims. *See Gov’t Br. 27*. The record reveals that Mr. Wilson’s involvement could generously be characterized as minimal, with Sgt. Alkire failing to even show him a copy of the second search warrant. Mr. Wilson’s guidance as to the second search warrant was confined to simply insisting that Sgt. Alkire “[j]ust do it.” J.A. 123.

Overall, the facts of this case are much closer to *Groh* than *Sheppard*. Here, Sgt. Alkire prepared an utterly facially deficient warrant without the strong reassurances by magistrates and prosecutors present in *Sheppard*. The second search warrant, which essentially provided for the indiscriminate rummaging through the contents of laptop, was “so facially deficient . . . that the executing officers [could not] reasonably presume it to be valid.” *Leon*, 668 U.S. at 923. As a result, Sgt. Alkire’s reliance on the warrant was not objectively reasonable. Therefore, the *Leon* good-faith exception to the exclusionary rule is inapplicable, so the child pornography should be suppressed.

### III.

Justice Frankfurter observed that, though “criminals have few friends,” the encroachment on the Fourth Amendment “reach[es] far beyond the thief or the blackmarketeer.” *Harris v. United States*, 331 U.S. 145, 156 (1947) (Frankfurter, J., dissenting). The encroachment in this case could reach anyone with a computer. By failing to persist in our historical commitment to the particularity requirement in this context, I

believe that the majority further opens the door to unrestricted searches of personal electronic devices. In today's modern world, such unrestricted searches are in many ways more invasive than the rifling of one's home. Because "I cannot give legal sanction to what was done in this case without accepting the implications of such a decision for the future," *id.*, I respectfully dissent.

# 12-240-cr

---

IN THE  
**United States Court of Appeals**  
FOR THE SECOND CIRCUIT

---

UNITED STATES OF AMERICA,

—against—

STAVROS M. GANIAS,

*Appellee,*

*Defendant-Appellant.*

ON APPEAL FROM THE UNITED STATES DISTRICT COURT  
FOR THE NEW HAVEN DISTRICT OF CONNECTICUT

---

**BRIEF FOR *AMICI CURIAE* CENTER FOR DEMOCRACY &  
TECHNOLOGY, AMERICAN CIVIL LIBERTIES UNION,  
AMERICAN CIVIL LIBERTIES UNION OF CONNECTICUT,  
BRENNAN CENTER FOR JUSTICE AT NYU SCHOOL OF LAW,  
ELECTRONIC FRONTIER FOUNDATION, AND  
NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE  
IN SUPPORT OF DEFENDANT-APPELLANT**

---

TANYA L. FORSHEIT  
BAKER & HOSTETLER LLP  
11601 Wilshire Boulevard, Suite 1400  
Los Angeles, California 90025  
(310) 442-8831  
tforsheit@bakerlaw.com

WILLIAM W. HELLMUTH  
BAKER & HOSTETLER LLP  
1050 Connecticut Avenue, NW, Suite 1100  
Washington, DC 20036  
(202) 861-1703  
whellmuth@bakerlaw.com

*Attorneys for Amicus Curiae  
Center for Democracy & Technology*

*(For Continuation of Appearances See Inside Cover)*

July 29, 2015

ALEX ABDO  
NATHAN FREED WESSLER  
JASON D. WILLIAMSON  
AMERICAN CIVIL LIBERTIES UNION  
FOUNDATION  
125 Broad Street, 18th Floor  
New York, New York 10004  
(212) 549-2500  
aabdo@aclu.org

DAN BARRETT  
AMERICAN CIVIL LIBERTIES UNION  
OF CONNECTICUT  
330 Main Street, 1st Floor  
Hartford, Connecticut 06106  
(860) 471-8471  
dbarrett@acluct.org  
\* Not admitted in Connecticut

FAIZA PATEL  
BRENNAN CENTER FOR JUSTICE  
AT NYU SCHOOL OF LAW  
161 Sixth Avenue, 12th Floor  
New York, New York 10013  
(646) 292-8335  
faiza.patel@nyu.edu

HANNI FAKHOURY  
ELECTRONIC FRONTIER FOUNDATION  
815 Eddy Street  
San Francisco, California 94109  
(415) 436-9333  
hanni@eff.org

LAURA M. MOY  
OPEN TECHNOLOGY INSTITUTE |  
NEW AMERICA  
1899 L Street, NW, Suite 400  
Washington, DC 20036  
(202) 986-2700  
moy@newamerica.org

*Attorneys for Amici Curiae*

## **CORPORATE DISCLOSURE STATEMENT**

Pursuant to Rules 26.1 and 29(c) of the Federal Rules of Appellate Procedure, *amici* state as follows:

The Center for Democracy and Technology has no parent company and has issued no stock. Thus, no publicly held corporation owns 10% or more of Center for Democracy and Technology stock.

The American Civil Liberties Union has no parent company and has issued no stock. Thus, no publicly held corporation owns 10% or more of American Civil Liberties Union stock.

The American Civil Liberties Union of Connecticut is an affiliate of the American Civil Liberties Union. No publicly held company owns 10% or more of its stock.

The Brennan Center for Justice is an institute affiliated with the New York University School of Law. No publicly held company owns 10% or more of its stock.

The Electronic Frontier Foundation has no parent company and has issued no stock. Thus, no publicly held corporation owns 10% or more of Electronic Frontier Foundation stock.

New America's Open Technology Institute is a program of New America. No publicly held company owns 10% or more of its stock.

**TABLE OF CONTENTS**

	<b>Page</b>
INTEREST OF AMICI CURIAE.....	1
SUMMARY OF ARGUMENT .....	5
ARGUMENT .....	7
I. The Copying of Digital Data Constitutes a Search and Seizure under the Fourth Amendment.....	7
II. The Retention of Digitally Copied Data Beyond the Scope of a Warrant is Unconstitutional under the Fourth Amendment. ....	12
III. The Court Should Decide the Constitutional Questions Presented Whether or Not It Determines that Suppression is Warranted. ....	20
CONCLUSION .....	22

**TABLE OF AUTHORITIES**

	<b>Page(s)</b>
<b>Cases</b>	
<i>ACLU v. Clapper</i> , 785 F.3d 787 (2d Cir. 2015) .....	2, 4
<i>Almeida v. Holder</i> , 588 F.3d 778 (2d Cir. 2009) .....	10
<i>Amnesty Int’l USA v. Clapper</i> , 638 F.3d 118 (2d Cir. 2011) .....	3
<i>Andresen v. Maryland</i> , 427 U.S. 463 (1976).....	13, 14, 18, 19
<i>Arizona v. Gant</i> , 556 U.S. 332 (2009).....	17
<i>Brigham City v. Stuart</i> , 547 U.S. 398 (2006).....	14
<i>Clapper v. Amnesty Int’l USA</i> , 133 S. Ct. 1138 (2013).....	2
<i>Davis v. United States</i> , 131 S. Ct. 2419 (2011).....	21
<i>eBay v. MercExchange, L.L.C.</i> , 547 U.S. 388 (2006).....	10
<i>Groh v. Ramirez</i> , 540 U.S. 551 (2004).....	14
<i>Hepting v. AT&amp;T Corp.</i> , 539 F.3d 1157 (9th Cir. 2008) .....	3
<i>Illinois v. Gates</i> , 462 U.S. 213 (1983).....	20, 21

*In the Matter of a Warrant to Search a Certain E-Mail Account  
Controlled and Maintained by Microsoft Corp.,  
15 F. Supp. 3d 466 (S.D.N.Y. 2014) ..... 1*

*In re Application of the U.S. For Historical Cell Site Data,  
724 F.3d 600 (5th Cir. 2013) .....4*

*In re Nat’l Sec. Agency Telecomms. Records Litig.,  
564 F. Supp. 2d 1109 (N.D. Cal. 2008).....3*

*Katz v. United States,  
389 U.S. 347 (1967).....8*

*Kyllo v. United States,  
533 U.S. 27 (2001).....8, 22*

*Leventhal v. Knapek,  
266 F.3d 64 (2d Cir. 2001) .....9*

*Loretto v. Teleprompter Manhattan CATV Corp.,  
458 U.S. 419 (1982)..... 11*

*Marron v. United States,  
275 U.S. 192 (1927).....12*

*Payton v. New York,  
445 U.S. 573 (1980).....17*

*Riley v. California,  
134 S. Ct. 2473 (2014).....*passim**

*Samson v. California,  
547 U.S. 843 (2006).....15*

*Soldal v. Cook Cnty.,  
506 U.S. 56 (1992).....11*

*United States v. Bach,  
310 F.3d 1063 (8th Cir. 2002) .....11*

*United States v. Clark,  
638 F.3d 89 (2d Cir. 2011) .....22*

*United States v. Comprehensive Drug Testing*,  
621 F.3d 1162 (9th Cir. 2010) .....11, 13, 14, 18

*United States v. Davis*,  
785 F.3d 498 (11th Cir. 2015) .....2, 4, 22

*United States v. Galpin*,  
720 F.3d 436 (2d Cir. 2013) .....16, 17, 18

*United States v. Ganas*,  
755 F.3d 125 (2d Cir. 2014) .....*passim*

*United States v. Jacobsen*,  
466 U.S. 109 (1984).....9

*United States v. Jones*,  
132 S. Ct. 945 (2012).....1, 2, 3, 4

*United States v. Karo*,  
468 U.S. 705 (1984).....10

*United States v. Katzin*,  
769 F.3d 163 (3d Cir. 2014) .....2

*United States v. Lifshitz*,  
369 F.3d 173 (2d Cir. 2004) .....9

*United States v. Martin*,  
157 F.3d 46 (2d Cir. 1998) .....16

*United States v. Otero*,  
563 F.3d 1127 (10th Cir. 2009) .....22

*United States v. Place*,  
462 U.S. 696 (1983).....11

*United States v. Warshak*,  
631 F.3d 266 (6th Cir. 2010) .....4, 21

*Virginia v. Moore*,  
553 U.S. 164 (2008).....15

*Watson v. Geren*,  
587 F.3d 156 (2d Cir. 2009) .....22

**Other Authorities**

Federal Rule of Appellate Procedure 35 .....22

Federal Rule of Criminal Procedure 41 .....4

Hon. James L. Oakes, “*Property Rights*” in *Constitutional Analysis*  
*Today*, 56 Wash. L. Rev. 583 (1981).....10

U.S. Const. amend. IV .....*passim*

## INTEREST OF *AMICI CURIAE*<sup>1</sup>

*Amici Curiae* are non-profit public interest organizations seeking to protect speech, privacy, and innovation—and access to speech and new technologies—on the Internet.

The Center for Democracy & Technology (CDT) is a non-profit public interest organization focused on privacy and other civil liberties issues affecting the Internet, other communications networks, and associated and emerging technologies. CDT represents the public's interest in an open Internet and promotes the constitutional and democratic values of free expression, privacy, and individual liberty in the digital world. It pursues that interest in the policy arena, and in the courts by filing briefs *amicus curiae* in cases that include *Riley v. California*, 134 S. Ct. 2473 (2014) (searches of cellular telephones incident to arrest); *United States v. Jones*, 132 S. Ct. 945 (2012) (warrantless GPS tracking involving physical trespass); and *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*, 15 F. Supp. 3d 466 (S.D.N.Y. 2014) (extraterritorial warrants).

---

<sup>1</sup> This amicus brief is filed with consent of the parties to this case. No party's counsel authored any portion of this brief, nor did any party or party's counsel contribute money intended to fund this brief's preparation or submission. No persons other than the *amici*, their members, or their counsel contributed money that was intended to fund this brief's preparation or submission.

The American Civil Liberties Union (“ACLU”) is a nationwide, nonprofit, nonpartisan organization with more than 500,000 members dedicated to the principles of liberty and equality embodied in the Constitution and this nation’s civil rights laws. The American Civil Liberties Union of Connecticut (“ACLU-CT”) is the affiliate of the ACLU in the State of Connecticut. Together and independently, the ACLU and the ACLU-CT have appeared numerous times before the federal courts in cases involving the Fourth Amendment, including, in particular, cases involving the right to privacy in the digital age. For example, the ACLU is or was counsel in *Clapper v. Amnesty Int’l USA*, 133 S. Ct. 1138 (2013) (FISA Amendments Act surveillance), *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015) (bulk collection of call records), and *United States v. Katzin*, 769 F.3d 163 (3d Cir. 2014) (warrantless GPS tracking), and it served as *amicus curiae* in *United States v. Jones*, 132 S. Ct. 945 (2012) (warrantless GPS tracking), *Riley v. California*, 134 S. Ct. 2473 (2014) (cellphone searches incident to arrest), and *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015) (warrantless acquisition of cellphone location information).

The Brennan Center for Justice at NYU School of Law is a non-partisan public policy and law institute focused on fundamental issues of democracy and justice, including access to the courts and constitutional limits on the government’s exercise of power. The Center’s Liberty and National Security (LNS) Program

uses innovative policy recommendations, litigation, and public advocacy to advance effective national security policies that respect the rule of law and constitutional values. The LNS Program is particularly concerned with domestic counterterrorism policies, including the dragnet collection of Americans' communications and personal data, and the concomitant effects on privacy and First and Fourth Amendment freedoms. As part of this effort, the Center has filed numerous amicus briefs on behalf of itself and others in cases involving electronic surveillance and privacy issues, including *Riley v. California*, 134 S. Ct. 2473 (2014); *United States v. Jones*, 132 S. Ct. 945 (2012); *Amnesty Int'l USA v. Clapper*, 638 F.3d 118 (2d Cir. 2011); *Hepting v. AT&T Corp.*, 539 F.3d 1157 (9th Cir. 2008); and *In re Nat'l Sec. Agency Telecomms. Records Litig.*, 564 F. Supp. 2d 1109 (N.D. Cal. 2008). The Brennan Center's views as amicus curiae in this case do not and will not purport to represent the position of NYU School of Law.

The Electronic Frontier Foundation ("EFF") is a member-supported civil liberties organization based in San Francisco, California, working to protect innovation, free speech, and privacy in a digital world. With more than 22,000 active donors nationwide, EFF represents the interests of technology users in both court cases and in broader policy debates surrounding the application of law in the digital age. As part of its mission, EFF has served as amicus curiae in landmark cases addressing Fourth Amendment issues raised by emerging technologies. *See*,

*e.g.*, *Riley v. California*, 134 S. Ct. 2473 (2014); *United States v. Jones*, 132 S. Ct. 945 (2012); *ACLU v. Clapper*, 785 F.3d 787 (2d Cir. 2015); *United States v. Davis*, 785 F.3d 498 (11th Cir. 2015) (en banc); *In re Application of the U.S. For Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013); *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

New America’s Open Technology Institute (“OTI”) is a program of New America dedicated to technology policy and technology development in support of digital rights, social justice, and universal access to open communications networks. OTI, through its unique blend of policy expertise, technical capacity, and field-level engagement, seeks to promote a stronger and more open Internet to support stronger and more open communities. Digital Fourth Amendment policy and law is a particular area of interest for OTI, and the Institute testifies before Congress regularly on issues of digital privacy and surveillance, as well as before the Judicial Conference Advisory Committee on Criminal Rules on the topic of Federal Rule of Criminal Procedure 41. New America is a non-profit civic enterprise dedicated to the renewal of American politics, prosperity, and purpose in the digital age through big ideas, technological innovation, next generation politics, and creative engagement with broad audiences.

## SUMMARY OF ARGUMENT

The Founders crafted the Fourth Amendment as a shield against unjustified or overreaching invasions into the privacy of individuals. In this case, the government threatens to upend that protection in the digital realm by ignoring key constitutional constraints on its authority to search or seize digital data. Specifically, the government argues that the Fourth Amendment permits it to seize vast quantities of data that has nothing to do with its investigation, to retain that data indefinitely, and to later search it in an entirely unrelated investigation. Taken to its logical conclusion, the government could amass a gigantic repository of every digital file it comes across that shares hard-drive space with files to which it is actually entitled, and then years later revisit people's most private personal records in aid of some new suspicion or case. This argument ignores the Fourth Amendment's requirements of particularity and reasonableness, and the Court should reject it. The Court should, instead, clarify two principles of law that would ensure that the Fourth Amendment's protections remain as robust in the digital world as they are in the physical world.

First, the Court should hold that the copying of digital data is a search and seizure under the Fourth Amendment. The circuit courts that have considered this question, including the panel in this case, have unanimously held as much, and for good reason. The copying of digital data places in government hands

extraordinarily sensitive information, in which individuals have a reasonable expectation of privacy. It also deprives the owner of critical possessory interests in the data: the exclusive use of it and the ability to delete it. Moreover, the copying of digital data by law enforcement serves precisely the same governmental purpose as any traditional search and seizure—namely, to secure evidence. A contrary rule—that the copying of digital data does not trigger the Fourth Amendment—would have devastating consequences for privacy by giving the government carte blanche to copy and store individuals’ data without any constitutional constraint.

Second, the Court should hold that, when the government seizes entire hard-drives of data to facilitate particularized searches, the Fourth Amendment forbids the government from retaining any non-responsive data for longer than reasonably necessary to effectuate its search. In this case, after copying several entire hard-drives of data, the government retained the data collected for an unreasonably long period of time, even after it had separated the data responsive to the original warrant from the non-responsive data. The government had no justifiable reason for retaining the nonresponsive data, and its retention was therefore unconstitutional under the Fourth Amendment.

The panel in this case noted that not only do “Fourth Amendment protections apply to modern computer files” but, “[i]f anything, even greater protection is warranted.” *United States v. Ganius*, 755 F.3d 125, 135 (2d Cir.

2014) (citations omitted). The Court should affirm these principles to ensure that, despite rapid changes in technology, the protections of the Fourth Amendment remain steadfast and strong.

## ARGUMENT

### **I. The Copying of Digital Data Constitutes a Search and Seizure under the Fourth Amendment.**

The panel opinion correctly held that the government’s copying of the defendant’s personal records “was a meaningful interference with [his] possessory rights in those files and constituted a seizure within the meaning of the Fourth Amendment.” *Ganias*, 755 F.3d at 137 (citations omitted). The Fourth Amendment provides that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. CONST. amend. IV. Here, the government’s copying of the defendant’s hard-drives triggered the Fourth Amendment for two independent reasons: (1) it was a search because it placed in government hands information in which the defendant had a reasonable expectation of privacy; and (2) it was a seizure because it deprived the defendant of the exclusive use of his records. This Court should affirm the panel’s conclusion—which is consistent

with the conclusion of every other circuit court to have addressed the question—that the copying of data triggers Fourth Amendment protections.

First, the copying of data constitutes a search within the meaning of the Fourth Amendment. In *Katz v. United States*, Justice Harlan stated in his concurring opinion that where “a person has a constitutionally protected reasonable expectation of privacy, . . . electronic as well as physical intrusion into a place that is in this sense private may constitute a violation of the Fourth Amendment.” 389 U.S. 347, 360 (1967) (Harlan, J., concurring). The courts have built upon Justice Harlan’s logic, and now recognize that “the ultimate touchstone of the Fourth Amendment is reasonableness.” *Riley v. California*, 134 S. Ct. 2473, 2482 (2014) (citations omitted). The Supreme Court has recognized that “a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable.” *Kyllo v. United States*, 533 U.S. 27, 33 (2001) (citing *Katz*, 389 U.S. at 361). Thus, a search within the meaning of the Fourth Amendment has occurred when law enforcement conducts an electronic intrusion into an environment where an individual has an actual expectation of privacy that society is prepared to recognize as reasonable.

The first question in this case, then, is whether the government invaded a reasonable expectation of privacy when it copied the entirety of Mr. Ganius’s hard-drives. It unquestionably did. Individuals reasonably expect that the government

will not take for its own purposes personal data stored privately on their computers. *See, e.g., United States v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) (“[i]ndividuals generally possess a reasonable expectation of privacy in their home computers” (collecting cases)). Further, in *Leventhal v. Knapek*, this Court concluded that an employee had a reasonable expectation of privacy in his personal files that were stored on his work computer. 266 F.3d 64, 72-74 (2d Cir. 2001). Here, Mr. Ganas likewise held a reasonable expectation of privacy in his files, particularly his personal files, which the government intruded upon when making the forensic copies of his computers.

There is no question that, had the government retained Mr. Ganas’s actual hard-drives, it would have invaded a reasonable expectation of privacy. There should also be no question that, when the government accomplishes the same ends by creating a mirror copy of the hard-drive, the government has likewise invaded a reasonable expectation of privacy.

Second, and independently, the copying of data constitutes a seizure within the meaning of the Fourth Amendment. “A ‘seizure’ of property occurs when there is some meaningful interference with an individual’s possessory interests in that property.” *United States v. Jacobsen*, 466 U.S. 109, 113 (1984) (citations omitted). The government’s copying of data interferes with at least two possessory interests: (1) the right to exclude others; and (2) the right to dispose of property.

As Justice Stevens wrote in *United States v. Karo*, “[t]he owner of property, of course, has a right to exclude from it all the world, including the government, and a concomitant right to use it exclusively for his own purposes.” 468 U.S. 705, 729 (1984) (Stevens, J., concurring in part, dissenting in part); *see also eBay v. MercExchange, L.L.C.*, 547 U.S. 388 (2006) (explaining that, in the patent infringement context, the essence of an ownership right is the right to exclude others from accessing a thing). And as this Court has observed more recently, “[t]he rights and benefits of property ownership . . . include not only the right to actual possession of a thing, but also the right to exclude others from possessing it, the right to use it and receive income from its use, the right to transmit it to another, and the right to sell, alienate, waste, or even destroy it.” *Almeida v. Holder*, 588 F.3d 778, 788 (2d Cir. 2009) (citing Hon. James L. Oakes, “*Property Rights*” in *Constitutional Analysis Today*, 56 Wash. L. Rev. 583, 589 (1981)).

The copying of digital data divests owners of these central possessory interests by preventing them from exercising absolute control over their data. It denies them the ability to exclude others from using their data, and it prevents them from disposing of their data as they see fit. Therefore, the act of copying this data meaningfully interferes with an individual’s possessory interests in the data, constituting a seizure under the Fourth Amendment.

The panel in this case reached this same conclusion. “Th[e] combination of circumstances [in this case] enabled the government to possess indefinitely personal records of Ganius that were beyond the scope of the warrant while it looked for other evidence to give it probable cause to search the files. This was a meaningful interference with Ganius’s possessory rights in those files and constituted a seizure within the meaning of the Fourth Amendment.” *Ganius*, 755 F.3d at 137 (citing *United States v. Place*, 462 U.S. 696, 708 (1983) (detaining a traveler’s luggage while awaiting the arrival of a drug-sniffing dog constituted a seizure); *Soldal v. Cook Cnty.*, 506 U.S. 56, 62-64, 68 (1992) (explaining that a seizure occurs when one’s property rights are violated, even if the property is never searched and the owner’s privacy was never violated); *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419, 435 (1982) (“The power to exclude has traditionally been considered one of the most treasured strands in an owner’s bundle of property rights.”)). Other circuits have reached similar conclusions. *See United States v. Comprehensive Drug Testing*, 621 F.3d 1162 (9th Cir. 2010) (en banc) (per curiam) (referring to the copying of electronic data as a seizure throughout the opinion); *United States v. Bach*, 310 F.3d 1063, 1065, 1067 (8th Cir. 2002) (describing information retrieved by the government with assistance of Yahoo! technicians from two email accounts as a “seizure”).

For these reasons, this Court should reaffirm the panel holding that the copying of digital data triggers ordinary Fourth Amendment protections. As explained more fully below, any other rule would have catastrophic consequences for privacy.

## **II. The Retention of Digitally Copied Data Beyond the Scope of a Warrant is Unconstitutional under the Fourth Amendment.**

Because the government's copying of Mr. Ganius's data constitutes a search or seizure under the Fourth Amendment, it must comply with the Fourth Amendment's warrant and reasonableness requirements. It did not in this instance.

First, the government retained data beyond the scope of its original warrant long after it had effectuated that warrant. As a general matter, the particularity requirement of the Fourth Amendment mandates that the government's searches and seizures be particular, or limited to the information, individuals, and places for which it can justify a search or seizure. *Marron v. United States*, 275 U.S. 192, 196 (1927) (“The requirement that warrants shall particularly describe the things to be seized makes general searches under them impossible and prevents the seizure of one thing under a warrant describing another. As to what is to be taken, nothing is left to the discretion of the officer executing the warrant.”).

In the digital context, courts have often permitted the government to *over-*seize data—that is, to seize data beyond the scope of its warrant—in order to facilitate its more targeted searches. Courts have permitted over-seizure as a

prophylactic to accommodate the government's claim that on-site review of digital data would be infeasible in certain circumstances.<sup>2</sup> *Comprehensive Drug Testing*, 621 F.3d at 1177 (recognizing "the reality that over-seizing is an inherent part of the electronic search process and [it will] proceed on the assumption that, when it comes to the seizure of electronic records, this will be far more common than in the days of paper records"); *see also Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976) (recognizing that over-seizure is sometimes appropriate, but cautioning against unwarranted intrusions into an individual's privacy). Even if the constitutional requirement of particularity permits that prophylactic, it does not permit the government to *profit* from it. The government may not convert that accommodation into a free license to retain data for which it would not independently have had probable cause to collect and search in the first place.

The Supreme Court has "long held . . . that the purpose of the particularity requirement is not limited to the prevention of general searches. . . . A particular warrant also assures the individual whose property is searched or seized of the

---

<sup>2</sup> Such a broad seizure may, itself, be unconstitutional, if there are narrower alternatives available. Indeed, given the severity of the invasion of the mirroring of a hard-drive, courts should insist upon clear evidence of the need for such a drastic measure. If they nonetheless approve of mirroring, courts should spell out the authority clearly in the warrant being issued, along with specific guidance and restrictions on the government's ability to search the media at issue and a clear statement on the government's obligation to promptly purge any data not within the scope of the warrant.

lawful authority of the executing officer, his need to search, and the limits of his power to search.” *Groh v. Ramirez*, 540 U.S. 551, 561 (2004) (citations omitted). Thus, in cases of electronic over-seizures, the government must limit its review and retention of computer files to those which it truly needs to search. *See Andresen*, 427 U.S. at 482 n.11; *Comprehensive Drug Testing*, 621 F.3d at 1177 (calling for “greater vigilance on the part of judicial officers in striking the right balance between the government’s interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures”). The government may not, in other words, read the particularity requirement out of the Constitution. To give that requirement meaning in the digital context, this Court should make clear that, when the government over-seizes digital data, it may not retain data unresponsive to its warrant beyond the full execution of its warrant or the time reasonably necessary to execute the warrant.

Second, even if the particularity requirement did not apply, the government’s retention of data unresponsive to its warrant long after it had effectuated that warrant would be unreasonable. “[T]he ultimate touchstone of the Fourth Amendment” is “reasonableness.” *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006). Reasonableness is determined by examining the “totality of the circumstances” to “assess[], on the one hand, the degree to which [government conduct] intrudes upon an individual’s privacy and, on the other, the degree to

which it is needed for the promotion of legitimate governmental interests.”

*Samson v. California*, 547 U.S. 843, 848 (2006) (quotation marks omitted); *see also Virginia v. Moore*, 553 U.S. 164, 171 (2008).

Here, the totality of the circumstances clearly demonstrates the unreasonableness of permitting the government to retain data long after it had effecuated its warrant. The government’s retention of Mr. Ganias’s records constituted a severe intrusion into the privacy of his papers, and the government had no legitimate interest in retaining data unresponsive to its warrant.

As a preliminary matter, it is uncontested that in 2004 the government was able to identify those materials from the seized computers that were responsive to the original warrant. Thus, the government created two distinct data sets: one set consisting of materials that were responsive to the 2003 warrant and a second set consisting of materials that were not responsive, but which contained Mr. Ganias’s personal files, among other documents. *Ganias*, 755 F.3d at 137-38. Mr. Ganias holds strong possessory and privacy interests in these files, particularly his personal files.

The government made a series of arguments as to why its retention and use of this nonresponsive data set was reasonable; however, as the panel noted, none of these arguments were persuasive. *See id.* at 138-40. Of the government’s arguments, only the claim that returning or destroying the non-responsive files

would compromise the remainder of the copied data appeared to demonstrate any actual interest in the non-responsive data set itself. *See id.* at 139. However, that rationale makes little sense: there ought to be any number of ways of preserving the evidentiary value of the responsive data seized without holding onto vast quantities of other data. As the panel stated, “[w]e are not convinced that there is no other way to preserve the evidentiary chain of custody. But even if we assumed it were necessary to maintain a complete copy of the hard-drive solely to authenticate evidence responsive to the original warrant, that does not provide a basis for using the mirror image for any other purpose.” *Id.*

Moreover, the government compounded the intrusion into Mr. Ganius’s personal data by retaining the data it seized for an additional one and a half years after it had fully executed its initial warrant, and by then searching the data yet again in an *unrelated* investigation. *See United States v. Martin*, 157 F.3d 46, 54 (2d Cir. 1998) (“[E]ven a seizure based on probable cause is unconstitutional if police act with unreasonable delay in securing a warrant.”).

Failure to recognize the copying of digital data by law enforcement as the equivalent of other forms of search and seizure would resurrect the “chief evil that prompted the framing and adoption of the Fourth Amendment”: permitting general warrants. *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013). As this Court explained in *Galpin*, the Fourth Amendment was adopted in response to “the

‘indiscriminate searches and seizures’ conducted by the British ‘under the authority of ‘general warrants.’” *Id.* (citing *Payton v. New York*, 445 U.S. 573, 583 (1980); *Arizona v. Gant*, 556 U.S. 332, 345 (2009) (“[T]he central concern underlying the Fourth Amendment [is] the concern about giving police officers unbridled discretion to rummage at will among a person’s private effects.”)). Therefore, a ruling that digital copying is not protected under the Fourth Amendment risks permitting unfettered gathering and warehousing of data by the government. It would enable the government to amass and maintain an enormous catalog of electronic communications and data that can later be reviewed if and when probable cause (or some other perceived justification) arises.

This is not an idle concern, particularly given the government’s posture in this case. Here, the government claimed that, after creating the mirror images of Mr. Ganius’s computers, those mirror images became “the government’s property,” which it was under no obligation to return or purge. *See Ganius*, 755 F.3d at 129. The government took this untenable position despite the fact that the mirror imaged copies are full of non-responsive (and almost certainly confidential and private) information, well outside the scope of the initial warrant under which the information was gathered. Going forward, as law enforcement copies more and more data in its investigations (in the cloud and beyond), this legal position will carry with it an ever greater threat to privacy in the digital age.

Moreover, the government's over-seizure of digital information is not unique to this case. It has frequently taken the position that the over-seizure of digital data is necessary to allow it to identify files and documents responsive to its warrants. *See, e.g., Galpin*, 720 F.3d at 447 (“As the Ninth Circuit has explained, because there is currently no way to ascertain the content of a file without opening it and because files containing evidence of a crime may be intermingled with millions of innocuous files, ‘[b]y necessity, government efforts to locate particular files will require examining a great many other files to exclude the possibility that the sought-after data are concealed there.’” (citing *Comprehensive Drug Testing, Inc.*, 621 F.3d at 1176)). It is quickly becoming the norm for the government to seize extraordinary amounts of digital data in the pursuit of narrow amounts of information. The government is poised, in other words, to create even more large stockpiles of information to be searched later, if and when needed, as it did in this case.

In *Andresen v. Maryland*, the Supreme Court recognized that there are “grave dangers inherent in executing a warrant authorizing a search and seizure of a person’s papers that are not necessarily present in executing a warrant to search for physical objects whose relevance is more easily ascertainable.” 427 U.S. at 482 n.11. These dangers are particularly present in executing warrants addressing digital information, where a search will implicate not only great volumes of

“papers,” but an unprecedented diversity of private information as well. *See Riley*, 134 S. Ct. at 2489 (“[A] cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record. [And] a cell phone’s capacity allows even just one type of information to convey far more than previously possible.”). Critically, the Supreme Court in *Andresen* observed that the “State was correct in returning [papers that were not within the scope of the warrants or were otherwise improperly seized] voluntarily [to the owner],” and that the “trial judge was correct in suppressing others.” 427 U.S. at 482 n.11. The Court cautioned that, when faced with searches and seizures of this scope, “responsible officials, including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.” *Id.*

Without a rule recognizing the copying of data as a search and seizure under the Fourth Amendment, the government might be tempted to gather information from individuals at its leisure, without a warrant, until such a time that the information might be needed. The end result of that would be a return to the very sort of activity that the Fourth Amendment was drafted to combat: indiscriminate collection of personal information by the government.

The government has failed to demonstrate a legitimate interest in retaining the non-responsive data set, let alone an interest sufficient to justify an intrusion into a constitutionally protected right. Once the government separated the responsive documents under the 2003 warrant from the non-responsive documents, the retention of the non-responsive documents became unreasonable and, as such, a violation of Mr. Ganas's Fourth Amendment rights.

### **III. The Court Should Decide the Constitutional Questions Presented Whether or Not It Determines that Suppression is Warranted.**

Regardless of whether suppression is ultimately warranted, this Court should address the novel and important Fourth Amendment questions raised in the instant case. An analysis of a good-faith reliance argument—which is an *exception* to the exclusionary rule—often requires courts to determine whether a Fourth Amendment violation occurred in the first place. *Illinois v. Gates*, 462 U.S. 213, 264-65 (1983) (White, J., concurring) (“Indeed, it may be difficult to determine whether the officers acted reasonably until the Fourth Amendment issue is resolved.”). But even if the Court *could* decide the case solely by addressing the good-faith exception to the exclusionary rule, it should not do so in light of the pressing need for judicial guidance on the underlying Fourth Amendment questions.

Federal, state, and local law enforcement agencies increasingly rely on searches of electronic devices, frequently carried out by making mirror image

copies of voluminous quantities of data. Yet, law enforcement agents and members of the public in this Circuit—as in others—lack guidance regarding the Fourth Amendment limits on such searches and the protections due to copied data once obtained. There is an acute need for guidance from this Court now, and that need will increase over time. Addressing the good-faith exception without also deciding the underlying Fourth Amendment question will deprive the public and the government of such guidance and result in “Fourth Amendment law . . . becoming ossified.” *Davis v. United States*, 131 S. Ct. 2419, 2433 (2011).

As the Sixth Circuit has explained:

If every court confronted with a novel Fourth Amendment question were to skip directly to good faith, the Government would be given *carte blanche* to violate constitutionally protected privacy rights, provided, of course, that a statute supposedly permits them to do so. The doctrine of good-faith reliance should not be a perpetual shield against the consequences of constitutional violations. In other words, if the exclusionary rule is to have any bite, courts must, from time to time, decide whether statutorily sanctioned conduct oversteps constitutional boundaries.

*United States v. Warshak*, 631 F.3d 266, 282 n.13 (6th Cir. 2010). Thus, “[w]hen a Fourth Amendment case presents a novel question of law whose resolution is necessary to guide future action by law enforcement officers and magistrates, there is sufficient reason for the Court to decide the violation issue *before* turning to the good-faith question.” *Gates*, 462 U.S. at 264 (White, J., concurring).

Indeed, the practice of reviewing substantive Fourth Amendment questions before turning to suppression or good faith is routine, including by this Court. *See*,

*e.g.*, *United States v. Clark*, 638 F.3d 89, 91 (2d Cir. 2011); *United States v. Otero*, 563 F.3d 1127, 1131–33 (10th Cir. 2009); *United States v. Davis*, 785 F.3d 498, 513, 518 n.20 (11th Cir. 2015) (en banc).

In granting *en banc* rehearing, this Court has already recognized the importance and novelty of the constitutional questions presented. *See* Fed. R. App. P. 35 (stating that *en banc* rehearing must not be ordered except where “the proceeding involves a question of exceptional importance”); *Watson v. Geren*, 587 F.3d 156, 160 (2d Cir. 2009) (“*En banc* review should be limited generally to only those cases that raise issues of important systemic consequences for the development of the law and the administration of justice.”). Because courts in this Circuit (and in others) are without guidance on Fourth Amendment questions surrounding the copying and retention of data, and because this area involves novel and important technological questions, the Court should decide the constitutionality of the search and seizure at issue. Doing so is necessary to ensure that technological advances do not “erode the privacy guaranteed by the Fourth Amendment.” *Kyllo*, 533 U.S. at 34.

## CONCLUSION

For the foregoing reasons, the Court should affirm that the copying of digital data constitutes a search and seizure under the Fourth Amendment and that the

government's retention and later search of Mr. Ganias's data that fell outside the scope of the 2003 subpoena was unconstitutional.

Dated: July 29, 2015

Respectfully submitted,  
/s/ William W. Hellmuth

Tanya L. Forsheit  
BAKER & HOSTETLER, LLP  
11601 Wilshire Boulevard, Suite 1400  
Los Angeles, California 90025  
(310) 442-8831  
tforsheit@bakerlaw.com

William W. Hellmuth  
BAKER & HOSTETLER, LLP  
1050 Connecticut Avenue, NW, Suite 1100  
Washington, DC 20036  
(202) 841-1059  
whellmuth@bakerlaw.com

*Counsel for Amicus Curiae The Center for  
Democracy and Technology*

Alex Abdo  
Nathan Freed Wessler  
Jason D. Williamson  
AMERICAN CIVIL LIBERTIES UNION  
FOUNDATION  
125 Broad Street, 18th Floor  
New York, NY 10004  
(212) 549-2500  
aabdo@aclu.org

Dan Barrett  
AMERICAN CIVIL LIBERTIES UNION OF  
CONNECTICUT  
330 Main Street, 1st Floor  
Hartford, CT 06106  
(860) 471-8471  
dbarrett@acluct.org  
\* Not admitted in Connecticut

Faiza Patel  
BRENNAN CENTER FOR JUSTICE AT NYU  
SCHOOL OF LAW  
161 Sixth Avenue, 12th Floor  
New York, New York 10013  
(646) 292-8335  
faiza.patel@nyu.edu

Hanni Fakhoury  
ELECTRONIC FRONTIER FOUNDATION  
815 Eddy Street  
San Francisco, California 94109  
(415) 436-9333  
hanni@eff.org

Laura M. Moy  
OPEN TECHNOLOGY INSTITUTE |  
NEW AMERICA  
1899 L Street, NW, Suite 400  
Washington, DC 20036  
(202) 986-2700  
moy@newamerica.org

## CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limitation of Fed. R. App. P 29(d) and Fed. R. App. P. 32(a)(7)(B) because it contains 5,445 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii). This brief complies with the typeface requirements of Fed. R. App. P 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in 14-point Times New Roman font.

Dated: July 29, 2015

/s/ William W. Hellmuth

William W. Hellmuth

BAKER & HOSTETLER, LLP  
1050 Connecticut Avenue, NW, Suite 1100  
Washington, DC 20036  
202) 841-1059  
whellmuth@bakerlaw.com

*Counsel for Amicus Curiae The Center for  
Democracy and Technology*

## CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Second Circuit by using the appellate CM/ECF system on July 29, 2015.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: July 29, 2015

/s/ William W. Hellmuth

William W. Hellmuth

BAKER & HOSTETLER, LLP  
1050 Connecticut Avenue, NW, Suite 1100  
Washington, DC 20036  
202) 841-1059  
whellmuth@bakerlaw.com

*Counsel for Amicus Curiae The Center for  
Democracy and Technology*

12-240-cr  
*United States v. Ganias*

UNITED STATES COURT OF APPEALS  
FOR THE SECOND CIRCUIT

August Term 2012

(Argued: April 11, 2013      Decided: June 17, 2014)

Docket No. 12-240-cr

---

UNITED STATES OF AMERICA,

*Appellee,*

v.

STAVROS M. GANIAS,

*Defendant-Appellant.*

---

Before:

HALL and CHIN, *Circuit Judges,*  
and RESTANI, *Judge.\**

---

Appeal from a judgment of the United States District Court for the  
District of Connecticut convicting defendant-appellant, following a jury trial, of

---

\* The Honorable Jane A. Restani, of the United States Court of International Trade, sitting by designation.

tax evasion. Defendant-appellant appeals on the grounds that: (1) the district court (Thompson, J.) erred in denying his motion to suppress his personal computer records, which had been retained by the Government for more than two-and-a-half years after it copied his computer hard drives pursuant to a search warrant calling for the seizure of his clients' business records; and (2) the district court (Burns, J.) abused its discretion in failing to order a new trial where a juror posted comments about the trial on his Facebook page and became Facebook friends with another juror during the trial. We find no abuse of discretion as to the second issue, but we conclude, however, that defendant-appellant's Fourth Amendment rights were violated by the unauthorized retention of his personal files. Accordingly, we vacate the judgment and remand for further proceedings.

VACATED and REMANDED.

Judge Hall concurs in part and dissents in part in a separate opinion.

---

SARALA V. NAGALA, Assistant United States Attorney  
(Anastasia E. King *and* Sandra S. Glover, Assistant  
United States Attorneys, *on the brief*), for David B.  
Fein, United States Attorney for the District of  
Connecticut, New Haven, Connecticut, *for*  
*Appellee*.

STANLEY A. TWARDY, JR. (Daniel E. Wenner, *on the brief*),  
Day Pitney LLP, Stamford, Connecticut, *for*  
*Defendant-Appellant.*

---

CHIN, *Circuit Judge*:

In this case, defendant-appellant Stavros M. Ganiias appeals from a judgment convicting him, following a jury trial, of tax evasion. He challenges the conviction on the grounds that his Fourth Amendment rights were violated when the Government copied three of his computer hard drives pursuant to a search warrant and then retained files beyond the scope of the warrant for more than two-and-a-half years. He also contends that his right to a fair trial was violated when, during the trial, a juror posted comments about the case on his Facebook page and "friended" another juror. We reject the second argument but hold that the Government's retention of the computer records was unreasonable.

Accordingly, we vacate the conviction and remand for further proceedings.

## STATEMENT OF THE CASE

### A. *The Facts*<sup>1</sup>

In the 1980s, after working for the Internal Revenue Service ("IRS") for some fourteen years, Ganas started his own accounting business in Wallingford, Connecticut. He provided tax and accounting services to individuals and small businesses. In 1998, he began providing services to James McCarthy and two of McCarthy's businesses, American Boiler and Industrial Property Management ("IPM"). IPM had been hired by the Army to provide maintenance and security at a vacant Army facility in Stratford, Connecticut.

In August 2003, the Criminal Investigative Command of the Army received a tip from a confidential source that individuals affiliated with IPM were engaging in improper conduct, including stealing copper wire and other items from the Army facility and billing the Army for work that IPM employees performed for American Boiler. The source alleged that evidence of the wrongdoing could be found at the offices of American Boiler and IPM, as well as

---

<sup>1</sup> The facts relevant to the issues on appeal are largely undisputed and are drawn from the testimony at the hearing on Ganas's motion to suppress, the decision of the district court (Thompson, *J.*) denying the suppression motion, and the transcript of the trial.

at the offices of "Steve Ganiis [sic]," who "perform[ed] accounting work for IPM and American Boiler."<sup>2</sup>

Based on this information, the Army commenced an investigation. Army investigators obtained several search warrants, including one to search the offices of Ganiis's accounting business. The warrant, issued by the United States District Court for the District of Connecticut and dated November 17, 2003, authorized the seizure from Ganiis's offices of:

All books, records, documents, materials, computer hardware and software and computer associated data relating to the business, financial and accounting operations of [IPM] and American Boiler . . . .

The warrant was executed two days later. Army computer specialists accompanied investigators to Ganiis's offices and helped gather the electronic evidence. The agents did not seize Ganiis's computers; instead, the computer specialists made identical copies, or forensic mirror images, of the hard drives of all three of Ganiis's computers. As a consequence, the investigators copied every file on all three computers -- including files beyond the scope of the warrant, such as files containing Ganiis's personal financial records. Ganiis was

---

<sup>2</sup> The record reflects that Ganiis, whose first name is Stavros, was often referred to as "Steve."

present as the investigators collected the evidence, and he expressed concern about the scope of the seizure. In response, one agent "assured" Ganas that the Army was only looking for files "related to American Boiler and IPM." Everything else, the agent explained, "would be purged once they completed their search" for relevant files.

Back in their offices, the Army computer specialist copied the data taken from Ganas's computers (as well as data obtained from the searches of the offices of IPM and American Boiler) onto "two sets of 19 DVDs," which were "maintained as evidence." Some eight months later, the Army Criminal Investigation Lab finally began to review the files.

In the meantime, while reviewing the paper documents retrieved from Ganas's offices, the Army discovered suspicious payments made by IPM to an unregistered business, which was allegedly owned by an individual who had not reported any income from that business. Based on this evidence, in May 2004, the Army invited the IRS to "join the investigation" of IPM and American Boiler and gave copies of the imaged hard drives to the IRS so that it could conduct its own review and analysis. The Army and the IRS proceeded, separately, to search the imaged hard drives for files that appeared to be within the scope of the warrant and to extract them for further review.

By December 2004, some thirteen months after the seizure, the Army and IRS investigators had isolated and extracted the computer files that were relevant to IPM and American Boiler and thus covered by the search warrant. The investigators were aware that, because of the constraints of the warrant, they were not permitted to review any other computer records. Indeed, the investigators were careful, at least until later, to review only data covered by the November 2003 warrant.

They did not, however, purge or delete the non-responsive files. To the contrary, the investigators retained the files because they "viewed the data as the government's property, not Mr. Ganius's property." Their view was that while items seized from an owner will be returned after an investigation closes, all of the electronic data here were evidence that were to be protected and preserved. As one agent testified, "[W]e would not routinely go into DVDs to delete data, as we're altering the original data that was seized. And you never know what data you may need in the future. . . . I don't normally go into electronic data and start deleting evidence off of DVDs stored in my evidence room." The computer specialists were never asked to delete (or even to try to delete) those files that did not relate to IPM or American Boiler.

In late 2004, IRS investigators discovered accounting irregularities regarding transactions between IPM and American Boiler in the paper documents taken from Ganias's office. After subpoenaing and reviewing the relevant bank records in 2005, they began to suspect that Ganias was not properly reporting American Boiler's income. Accordingly, on July 28, 2005, some twenty months after the seizure of his computer files, the Government officially expanded its investigation to include possible tax violations by Ganias. Further investigation in 2005 and early 2006 indicated that Ganias had been improperly reporting income for both of his clients, leading the Government to suspect that he also might have been underreporting his own income.

At that point, the IRS case agent wanted to review Ganias's personal financial records and she knew, from her review of the seized computer records, that they were among the files in the DVDs copied from Ganias's hard drives. The case agent was aware, however, that Ganias's personal financial records were beyond the scope of the November 2003 warrant, and consequently she did not believe that she could review the non-responsive files, even though they were already in the Government's possession.

In February 2006, the Government asked Ganas and his counsel for permission to access certain of his personal files that were contained in the materials seized in November 2003. Ganas did not respond, and thus, on April 24, 2006, the Government obtained another warrant to search the preserved images of Ganas's personal financial records taken in 2003. At that point, the images had been in the Government's possession for almost two-and-a-half years. Because Ganas had altered the original files shortly after the Army executed the 2003 warrant, the evidence obtained in 2006 would not have existed but for the Government's retention of those images.

**B. *Procedural History***

**1. *The Indictment***

In October 2008, a grand jury indicted Ganas and McCarthy for conspiracy and tax evasion. The grand jury returned a superseding indictment in December 2009, containing certain counts relating to McCarthy's taxes and two counts relating to Ganas's personal taxes. The latter two counts were asserted only against Ganas. The case was assigned to Chief Judge Alvin W. Thompson.

**2. *The Motion to Suppress***

In February 2010, Ganas moved to suppress the computer files that are the subject of this appeal. In April 2010, the district court (Thompson, *J.*) held

a two-day hearing and, on April 14, 2010, it denied the motion, with an indication that a written decision would follow. On June 24, 2011, the district court filed its written decision explaining the denial of Ganias's motion to suppress. *See United States v. Ganias*, No. 3:08 Cr. 224, 2011 WL 2532396 (D. Conn. June 24, 2011).

### 3. *The Trial*

In April 2010, the case was transferred to Judge Ellen Bree Burns for trial. In May 2010, the district court severed the two counts against Ganias for tax evasion with respect to his personal taxes from the other charges.<sup>3</sup>

Trial commenced on March 8, 2011, with jury selection, and testimony was scheduled to begin on March 10, 2011. At 9:34 p.m. on March 9, the evening before the start of the evidence, one of the jurors, Juror X, posted a comment on his Facebook page: "Jury duty 2morrow. I may get 2 hang someone...can't wait."

Juror X's posting prompted responses from some of his online "friends," including: "gettem while the're young !!!...lol" and "let's not be to hasty. Torcher first, then hang! Lol." During the trial, Juror X continued to post comments about his jury service, including:

---

<sup>3</sup> All the other counts were later dismissed.

March 10 at 3:34 pm:

Shit just told this case could last 2 weeks..  
Jury duty sucks!

March 15 at 1:41 pm:

Your honor I object! This is way too  
boring.. somebody get me outta here.

March 17 at 2:07 pm:

Guinness for lunch break. Jury duty ok  
today.

During the second week of trial, Juror X became Facebook friends with another one of the jurors.

On April 1, 2011, the jury convicted Ganas on both counts. Later that evening, at 9:49 pm, Juror X posted another comment on his Facebook page:

"GUILTY:)." He later elaborated:

I spent the whole month of March in court. I do believe justice prevailed! It was no cake walk getting to the end! I am glad it is over and I have a new experience under my belt!

#### **4. *The Motion for a New Trial***

On August 17, 2011, Ganas moved for a new trial based on alleged juror misconduct. On August 30, 2011, the district court (Burns, J.) held an

evidentiary hearing and took testimony from Juror X. The district court denied the motion (as well as a request for the further taking of evidence) in a decision filed on October 5, 2011. *See United States v. Ganius*, No. 3:08 Cr. 224, 2011 WL 4738684 (D. Conn. Oct. 5, 2011).

At the post-trial evidentiary hearing, Juror X explained that he posted the comment on his Facebook page about "hang[ing] someone" as "a joke, all friend stuff," and that he was "[j]ust joking, joking around." At first he could not recall whether he had any conversations with the other juror, with whom he became Facebook friends during the trial, outside the court. He later clarified, however, that he did not have any conversations with the other juror during the course of the trial, prior to deliberations, about the subject matter of the case. He also testified that he in fact considered the case fairly and impartially. The district court accepted Juror X's testimony, found that he was credible, and concluded that he had participated in the deliberations impartially and in good faith.

## 5. *Sentencing*

On January 5, 2012, the district court (Burns, J.) sentenced Ganius principally to twenty-four months' imprisonment. This appeal followed. Ganius was released pending appeal.

## *DISCUSSION*

Ganias raises two issues on appeal: first, he contends that his Fourth Amendment rights were violated when the Government seized his personal computer records and then retained them for more than two-and-a-half years; and, second, he contends that he was entitled to a new trial because of the jury's improper use of social media.

As to the Fourth Amendment issue, we review the district court's findings of fact for clear error, viewing the evidence in the light most favorable to the Government, and its conclusions of law *de novo*. *United States v. Ramos*, 685 F.3d 120, 128 (2d Cir.), *cert. denied*, 133 S. Ct. 567 (2012). As to the issue of the district court's denial of Ganias's motion for a new trial for alleged juror misconduct, we review for abuse of discretion. *United States v. Farhane*, 634 F.3d 127, 168 (2d Cir.), *cert. denied*, 132 S. Ct. 833 (2011).

Although we vacate Ganias's conviction on the Fourth Amendment grounds, we address his juror misconduct claim because the increasing popularity of social media warrants consideration of this question. We address the juror misconduct question first, as it presents less difficult legal issues, and we then turn to the Fourth Amendment question.

**A. Juror's Improper Use of Social Media**

**1. Applicable Law**

Defendants have the right to a trial "by an impartial jury." U.S. Const. amend. VI. That right is not violated, however, merely because a juror places himself in a "potentially compromising situation." *United States v. Aiello*, 771 F.2d 621, 629 (2d Cir. 1985), *abrogated on other grounds by Rutledge v. United States*, 517 U.S. 292 (1996); *see also Smith v. Phillips*, 455 U.S. 209, 217 (1982) ("[I]t is virtually impossible to shield jurors from every contact or influence that might theoretically affect their vote."). A new trial will be granted only if "the juror's ability to perform her duty impartially has been adversely affected," *Aiello*, 771 F.2d at 629, and the defendant has been "substantially prejudiced" as a result, *United States v. Fumo*, 655 F.3d 288, 305 (3d Cir. 2011). Although courts are understandably reluctant to invade the sanctity of the jury's deliberations, the trial judge should inquire into a juror's partiality where there are reasonable grounds to believe the defendant may have been prejudiced. *United States v. Schwarz*, 283 F.3d 76, 97 (2d Cir. 2002); *United States v. Sun Myung Moon*, 718 F.2d 1210, 1234 (2d Cir. 1983). That inquiry should end, however, as soon as it becomes apparent that those reasonable grounds no longer exist. *See Sun Myung Moon*, 718 F.2d at 1234.

**B. *Application***

A juror who "friends" his fellow jurors on Facebook, or who posts comments about the trial on Facebook, may, in certain circumstances, threaten a defendant's Sixth Amendment right to an impartial jury.<sup>4</sup> Those circumstances, however, are not present here. The district court inquired into the matter and credited Juror X's testimony that he deliberated impartially and in good faith. The district judge's credibility determination was not clearly erroneous, and thus she did not abuse her discretion in denying the motion for a new trial.

This case demonstrates, however, that vigilance on the part of trial judges is warranted to address the risks associated with jurors' use of social media. The Third Circuit has endorsed the use of jury instructions like those proposed by the Judicial Conference Committee on Court Administration and Case Management. *See Fumo*, 655 F.3d at 304-05. We do so as well.

---

<sup>4</sup> *See, e.g., Fumo*, 655 F.3d at 331 (Nygaard, J., concurring) ("The availability of the Internet and the abiding presence of social networking now dwarf the previously held concern that a juror may be exposed to a newspaper article or television program."); *United States v. Juror Number One*, 866 F. Supp. 2d 442, 451 (E.D. Pa. 2011) ("[T]he extensive use of social networking sites, such as Twitter and Facebook, have exponentially increased the risk of prejudicial communication amongst jurors and opportunities to exercise persuasion and influence upon jurors."). *See generally* Amy J. St. Eve & Michael A. Zuckerman, *Ensuring an Impartial Jury in the Age of Social Media*, 11 Duke L. & Tech. Rev. 1 (2012).

The Committee proposes that, before trial, the district judge give an instruction that includes the following:

I know that many of you use cell phones, Blackberries, the internet and other tools of technology. You also must not talk to anyone about this case or use these tools to communicate electronically with anyone about the case. This includes your family and friends. You may not communicate with anyone about the case on your cell phone, through e-mail, Blackberry, iPhone, text messaging, or on Twitter, through any blog or website, through any internet chat room, or by way of any other social networking websites, including Facebook, My Space, LinkedIn, and YouTube.<sup>5</sup>

The Committee also recommends giving a similar instruction at the close of the case:

During your deliberations, you must not communicate with or provide any information to anyone by any means about this case. You may not use any electronic device or media, such as a telephone, cell phone, smart phone, iPhone, Blackberry or computer; the internet, or any internet service, or any text or instant messaging service; or any internet chat room, blog, or website, such as Facebook, My Space, LinkedIn,

---

<sup>5</sup> Judicial Conference Comm. on Court Admin. & Case Mgmt., Proposed Model Jury Instructions: The Use of Electronic Technology to Conduct Research on or Communicate about a Case (December 2009), *available at* [www.uscourts.gov/uscourts/News/2010/docs/DIR10-018-Attachment.pdf](http://www.uscourts.gov/uscourts/News/2010/docs/DIR10-018-Attachment.pdf).

YouTube or Twitter, to communicate to anyone any information about this case or to conduct any research about this case until I accept your verdict.<sup>6</sup>

Here, while the district court gave an appropriate instruction at the start of the jury's deliberations, it does not appear that it did so earlier. As demonstrated by this case, instructions at the beginning of deliberations may not be enough. We think it would be wise for trial judges to give the Committee's proposed instructions both at the start of trial and as deliberations begin, and to issue similar reminders throughout the trial before dismissing the jury each day. While situations like the one in this case will not always require a new trial, it is the better practice for trial judges to be proactive in warning jurors about the risks attending their use of social media.

**B. *The Seizure and Retention of Ganias's Computer Records***

**1. *Applicable Law***

The Fourth Amendment protects the rights of individuals "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV; *see, e.g., United States v. Ramirez*, 523 U.S. 65, 71 (1998). A search occurs when the Government acquires

---

<sup>6</sup> *Id.*

information by either "physically intruding on persons, houses, papers, or effects," or otherwise invading an area in which the individual has a reasonable expectation of privacy. *See Florida v. Jardines*, 133 S. Ct. 1409, 1414 (2013) (internal quotation mark omitted); *see also Katz v. United States*, 389 U.S. 347, 360-61 (1967) (Harlan, J., concurring). A seizure occurs when the Government interferes in some meaningful way with the individual's possession of property. *United States v. Jones*, 132 S. Ct. 945, 951 n.5 (2012). Subject to limited exceptions,<sup>7</sup> a search or seizure conducted without a warrant is presumptively unreasonable. *See Kyllo v. United States*, 533 U.S. 27, 31 (2001).

We must construe the Fourth Amendment "in [] light of what was deemed an unreasonable search and seizure when it was adopted, and in a manner which will conserve public interests as well as the interests and rights of individual citizens." *Kyllo*, 533 U.S. at 40. Applying 18th Century notions about searches and seizures to modern technology, however, is easier said than done, as we are asked to measure Government actions taken in the "computer age" against Fourth Amendment frameworks crafted long before this technology

---

<sup>7</sup> In this case, the Government has conceded that it needed a warrant to search the non-responsive computer files in its possession and has not argued that any exceptions apply.

existed.<sup>8</sup> As we do so, we must keep in mind that "the ultimate touchstone of the Fourth Amendment is reasonableness." *Missouri v. McNeely*, 133 S. Ct. 1552, 1569 (2013) (Roberts, C.J., concurring in part and dissenting in part) (internal quotation marks omitted). Because the degree of privacy secured to citizens by the Fourth Amendment has been impacted by the advance of technology, the challenge is to adapt traditional Fourth Amendment concepts to the Government's modern, more sophisticated investigative tools.

"The chief evil that prompted the framing and adoption of the Fourth Amendment was the 'indiscriminate searches and seizures' conducted by the British 'under the authority of general warrants.'" *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) (quoting *Payton v. New York*, 445 U.S. 573, 583 (1980)) (internal quotation marks omitted). General warrants were ones "not grounded upon a sworn oath of a specific infraction by a particular individual, and thus not

---

<sup>8</sup> See generally *United States v. Jones*, 132 S. Ct. 945 (2012) (considering whether placing GPS tracking unit on vehicle constitutes search); *Kyllo*, 533 U.S. at 27 (determining whether use of thermal imaging constitutes search); *United States v. Aguiar*, 737 F.3d 251 (2d Cir. 2013) (determining whether warrantless placement of GPS tracking unit on vehicle fell within good-faith exception to exclusionary rule); *United States v. Galpin*, 720 F.3d 436 (2d Cir. 2013) (analyzing whether warrant to search computer satisfies particularity requirement); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531 (2005); James Saylor, Note, *Computers as Castles: Preventing the Plain View Doctrine from Becoming a Vehicle for Overbroad Digital Searches*, 79 Fordham L. Rev. 2809 (2011); Marc Palumbo, Note, *How Safe Is Your Data?: Conceptualizing Hard Drives Under the Fourth Amendment*, 36 Fordham Urb. L.J. 977 (2009).

limited in scope and application." *Maryland v. King*, 133 S. Ct. 1958, 1980 (2013).

The British Crown had long used these questionable instruments to enter a political opponent's home and seize all his books and papers, hoping to find among them evidence of criminal activity. *See Stanford v. Texas*, 379 U.S. 476, 482-83 (1965). The Framers abhorred this practice, believing that "papers are often the dearest property a man can have" and that permitting the Government to "sweep away all papers whatsoever," without any legal justification, "would destroy all the comforts of society." *Entick v. Carrington*, 95 Eng. Rep. 807, 817-18 (C.P. 1765).<sup>9</sup>

The Fourth Amendment guards against this practice by providing that a warrant will issue only if: (1) the Government establishes probable cause to believe the search will uncover evidence of a specific crime; and (2) the warrant states with particularity the areas to be searched and the items to be seized. *Galpin*, 720 F.3d at 445. The latter requirement, in particular, "makes general searches . . . impossible" because it "prevents the seizure of one thing

---

<sup>9</sup> The Supreme Court has explained that *Entick* was "undoubtedly familiar to every American statesman at the time the Constitution was adopted, and considered to be the true and ultimate expression of constitutional law with regard to search and seizure." *Jones*, 132 S. Ct. at 949 (internal quotation marks omitted).

under a warrant describing another." *Id.* at 446 (quoting *Marron v. United States*, 275 U.S. 192, 196 (1927)) (internal quotation marks omitted). This restricts the Government's ability to remove all of an individual's papers for later examination because it is generally unconstitutional to seize any item not described in the warrant. *See Horton v. California*, 496 U.S. 128, 140 (1990); *United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982). Certain exceptions have been made in those "comparatively rare instances where documents [we]re so intermingled that they [could not] feasibly be sorted on site." *Tamura*, 694 F.2d at 595-96. But in those cases, the off-site review had to be monitored by a neutral magistrate and non-responsive documents were to be returned after the relevant items were identified. *Id.* at 596-97.

These Fourth Amendment protections apply to modern computer files. Like 18th Century "papers," computer files may contain intimate details regarding an individual's thoughts, beliefs, and lifestyle, and they should be similarly guarded against unwarranted Government intrusion. If anything, even greater protection is warranted. *See, e.g., Galpin*, 720 F.3d at 446 ("[A]dvances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and

quantity of private information it may contain."); *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009) ("The modern development of the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs . . . ."); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 569 (2005) (explaining that computers have become the equivalent of "postal services, playgrounds, jukeboxes, dating services, movie theaters, daily planners, shopping malls, personal secretaries, virtual diaries, and more").

Not surprisingly, the ability of computers to store massive volumes of information presents logistical problems in the execution of search warrants. It is "comparatively" commonplace for files on a computer hard drive to be "so intermingled that they cannot feasibly be sorted on site." *Tamura*, 694 F.2d at 595. As evidenced by this case, forensic analysis of electronic data may take months to complete. It would be impractical for agents to occupy an individual's home or office, or seize an individual's computer, for such long periods of time. It is now also unnecessary. Today, advancements in technology enable the Government to create a mirror image of an individual's hard drive, which can be searched as if it

were the actual hard drive but without interfering with the individual's use of his home, computer, or files.

In light of the significant burdens on-site review would place on both the individual and the Government, the creation of mirror images for off-site review is constitutionally permissible in most instances, even if wholesale removal of tangible papers would not be. Indeed, the 2009 amendments to the Federal Rules of Criminal Procedure, which added Rule 41(e)(2)(B), clearly contemplated off-site review of computer hard drives in certain circumstances.<sup>10</sup> Although Rule 41(e)(2)(B) was not in effect in 2003, when the warrant was executed with respect to Ganius's computers, case law both before and after the rule's adoption has recognized that off-site review of seized electronic files may

---

<sup>10</sup> Rule 41(e)(2)(B) provides:

**Warrant Seeking Electronically Stored Information.**

A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.

Fed. R. Crim. P. 41(e)(2)(B).

be necessary and reasonable. *See, e.g., United States v. Schesso*, 730 F.3d 1040, 1046 (9th Cir. 2013); *United States v. Evers*, 669 F.3d 645, 652 (6th Cir. 2012); *United States v. Hill*, 459 F.3d 966, 976-77 (9th Cir. 2006); *United States v. Upham*, 168 F.3d 532, 535 (1st Cir. 1999).

The off-site review of these mirror images, however, is still subject to the rule of reasonableness. *See, e.g., Ramirez*, 523 U.S. at 71 ("The general touchstone of reasonableness which governs Fourth Amendment analysis governs the method of execution of the warrant." (citation omitted)). The advisory committee's notes to the 2009 amendment of the Federal Rules of Criminal Procedure shed some light on what is "reasonable" in this context. Specifically, the committee rejected "a presumptive national or uniform time period within which any subsequent off-site copying or review of the media or electronically stored information would take place." Fed. R. Crim. P. 41(e)(2)(B) advisory committee's notes to the 2009 Amendments. The committee noted that several variables -- storage capacity of media, difficulties created by encryption or electronic booby traps, and computer-lab workload -- influence the duration of a forensic analysis and counsel against a "one size fits all" time period. *Id.* In combination, these factors might justify an off-site review lasting for a significant

period of time. They do not, however, provide an "independent basis" for retaining any electronic data "other than [those] specified in the warrant." *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1171 (9th Cir. 2010) (en banc).

Even where a search or seizure violates the Fourth Amendment, the Government is not automatically precluded from using the unlawfully obtained evidence in a criminal prosecution. *United States v. Julius*, 610 F.3d 60, 66 (2d Cir. 2010). "To trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system." *Herring v. United States*, 555 U.S. 135, 144 (2009). Suppression is required "only when [agents] (1) . . . effect a widespread seizure of items that were not within the scope of the warrant, and (2) do not act in good faith." *United States v. Shi Yan Liu*, 239 F.3d 138, 140 (2d Cir. 2000) (internal quotation marks and citations omitted).

The Government effects a "widespread seizure of items" beyond the scope of the warrant when the Government's search "resemble[s] a general search." *Id.* at 140-41. Government agents act in good faith when they perform "searches conducted in objectively reasonable reliance on binding appellate

precedent." *Davis v. United States*, 131 S. Ct. 2419, 2423-24 (2011). When Government agents act on "good-faith reliance [o]n the law at the time of the search," the exclusionary rule will not apply. *United States v. Aguiar*, 737 F.3d 251, 259 (2d Cir. 2013). "The burden is on the government to demonstrate the objective reasonableness of the officers' good faith reliance." *United States v. Voustianiouk*, 685 F.3d 206, 215 (2d Cir. 2012) (internal quotation marks omitted).

Furthermore, evidence will be suppressed only where the benefits of deterring the Government's unlawful actions appreciably outweigh the costs of suppressing the evidence -- "a high obstacle for those urging . . . application" of the rule. *Herring*, 555 U.S. at 141; see *Pennsylvania Bd. of Prob. & Parole v. Scott*, 524 U.S. 357, 364-65 (1998) (citing *United States v. Payner*, 447 U.S. 727, 734 (1980)). "The principal cost of applying the [exclusionary] rule is, of course, letting guilty and possibly dangerous defendants go free -- something that 'offends basic concepts of the criminal justice system.'" *Herring*, 555 U.S. at 141 (quoting *United States v. Leon*, 468 U.S. 897, 908 (1984)).

## **2. Analysis**

This case presents a host of challenging issues, but we need not address them all. The parties agree that the personal financial records at issue in

this appeal were not covered by the 2003 warrant, and that they had been segregated from the responsive files by December 2004, before the Government began to suspect that Ganas was personally involved in any criminal activity. Furthermore, on appeal, Ganas does not directly challenge the Government's practice of making mirror images of computer hard drives when searching for electronic data, but rather challenges the reasonableness of its off-site review. Accordingly, we need not address whether: (1) the description of the computer files to be seized in the 2003 warrant was stated with sufficient particularity, *see, e.g., Galpin*, 720 F.3d at 449-50; (2) the 2003 warrant authorized the Government to make a mirror image of the entire hard drive so it could search for relevant files off-site; or (3) the resulting off-site sorting process was unreasonably long.

Instead, we consider a more limited question: whether the Fourth Amendment permits officials executing a warrant for the seizure of particular data on a computer to seize and indefinitely retain every file on that computer for use in future criminal investigations. We hold that it does not.

If the 2003 warrant authorized the Government to retain all the data on Ganas's computers on the off-chance the information would become relevant to a subsequent criminal investigation, it would be the equivalent of a general

warrant. The Government's retention of copies of Ganas's personal computer records for two-and-a-half years deprived him of exclusive control over those files for an unreasonable amount of time. This combination of circumstances enabled the Government to possess indefinitely personal records of Ganas that were beyond the scope of the warrant while it looked for other evidence to give it probable cause to search the files. This was a meaningful interference with Ganas's possessory rights in those files and constituted a seizure within the meaning of the Fourth Amendment. *See United States v. Place*, 462 U.S. 696, 708 (1983) (detaining a traveler's luggage while awaiting the arrival of a drug-sniffing dog constituted a seizure); *see also Soldal v. Cook Cnty.*, 506 U.S. 56, 62-64, 68 (1992) (explaining that a seizure occurs when one's property rights are violated, even if the property is never searched and the owner's privacy was never violated); *Loretto v. Teleprompter Manhattan CATV Corp.*, 458 U.S. 419, 435 (1982) ("The power to exclude has traditionally been considered one of the most treasured strands in an owner's bundle of property rights.").

We conclude that the unauthorized seizure and retention of these documents was unreasonable. The Government had no warrant authorizing the seizure of Ganas's personal records in 2003. By December 2004, these documents

had been separated from those relevant to the investigation of American Boiler and IPM. Nevertheless, the Government continued to retain them for another year-and-a-half until it finally developed probable cause to search and seize them in 2006. Without some independent basis for its retention of those documents in the interim, the Government clearly violated Ganas's Fourth Amendment rights by retaining the files for a prolonged period of time and then using them in a future criminal investigation.

The Government offers several arguments to justify its actions, but none provides any legal authorization for its continued and prolonged possession of the non-responsive files. First, it argues that it must be allowed to make the mirror image copies as a matter of practical necessity and, according to the Government's investigators, those mirror images were "the government's property." As explained above, practical considerations may well justify a reasonable accommodation in the manner of executing a search warrant, such as making mirror images of hard drives and permitting off-site review, but these considerations do not justify the indefinite retention of non-responsive documents. *See Comprehensive Drug Testing, Inc.*, 621 F.3d at 1171. Without a warrant authorizing seizure of Ganas's personal financial records, the copies of

those documents could not become *ipso facto* "the government's property" without running afoul of the Fourth Amendment.

Second, the Government asserts that by obtaining the 2006 search warrant, it cured any defect in its search of the wrongfully retained files. But this argument "reduces the Fourth Amendment to a form of words." *Silverthorne Lumber Co. v. United States*, 251 U.S. 385, 392 (1920). In *Silverthorne*, the Government, "without a shadow of authority[,] went to the office of [the defendants'] company and made a clean sweep of all the books, papers and documents found there." *Id.* at 390. The originals were eventually returned because they were unlawfully seized, but the prosecutor had made "[p]hotographs and copies of material papers" and used these to indict the defendants and obtain a subpoena for the original documents. *Id.* at 391. Justice Holmes succinctly summarized the Government's argument supporting the constitutionality of its actions as follows:

[A]lthough of course its seizure was an outrage which the Government now regrets, it may study the papers before it returns them, copy them, and then may use the knowledge that it has gained to call upon the owners in a more regular form to produce them; that the protection of the Constitution covers the physical possession but

not any advantages that the Government can gain over the object of its pursuit by doing the forbidden act.

*Id.* Unsurprisingly, the Supreme Court rejected that argument: "The essence of a provision forbidding the acquisition of evidence in a certain way is that not merely evidence so acquired shall not be used before the Court but that it shall not be used at all" unless some exception applies.<sup>11</sup> *Id.* at 392. The same rationale applies here. If the Government could seize and retain non-responsive electronic records indefinitely, so it could search them whenever it later developed probable cause, every warrant to search for particular electronic data would become, in essence, a general warrant.

Third, the Government argues that it must be permitted to search the

---

<sup>11</sup> The Supreme Court has abrogated *Silverthorne's* broad proposition that wrongfully acquired evidence may "not be used at all." See *United States v. Havens*, 446 U.S. 620, 624-25 (1980) (noting that this evidence may be used for purposes of impeachment); see also *Murray v. United States*, 487 U.S. 533, 537 (1988) (explaining that the "independent source" doctrine allows the admission of "evidence initially discovered during, or as a consequence of, an unlawful search, but later obtained independently from activities untainted by the initial illegality"); *Nix v. Williams*, 467 U.S. 431, 444 (1984) (explaining that "inevitable discovery" doctrine permits the admission of unlawfully obtained evidence if "th[at] information ultimately or inevitably would have been discovered by lawful means"). The Government does not rely on any of these exceptions here. Indeed, it concedes that if it "had not preserved that data from the November 2003 seizure, it would have been lost forever." Appellee's Br. at 33. We do not hold that the Government has waived its right to use the evidence in question for impeachment purposes.

mirror images in its possession because the evidence no longer existed on Ganas's computers. But the ends, however, do not justify the means. The loss of the personal records is irrelevant in this case because the Government concedes that it never considered performing a new search of Ganas's computers and did not know that the files no longer existed when it searched the mirror images in its possession. And even if it were relevant, the Fourth Amendment clearly embodies a judgment that some evidence of criminal activity may be lost for the sake of protecting property and privacy rights. *See, e.g., United States v. Calandra*, 414 U.S. 338, 361 (1974) ("The judges who developed the exclusionary rule were well aware that it embodied a judgment that it is better for some guilty persons to go free than for the [Government] to behave in forbidden fashion.").

Fourth, the Government contends that returning or destroying the non-responsive files is "entirely impractical" because doing so would compromise the remaining data that was responsive to the warrant, making it impossible to authenticate or use it in a criminal prosecution. Appellee Br. at 34. We are not convinced that there is no other way to preserve the evidentiary chain of custody. But even if we assumed it were necessary to maintain a complete copy of the hard drive solely to authenticate evidence responsive to the original

warrant, that does not provide a basis for using the mirror image for any other purpose.

Finally, the Government argues that Ganias's failure to bring a motion for the return of property, pursuant to Federal Rule of Criminal Procedure 41(g), precludes him from seeking suppression now. Although the district court accepted this argument, we find no authority for concluding that a Rule 41(g) motion is a prerequisite to a motion to suppress. *See* Fed. R. Crim. P. 41(g) ("A person aggrieved . . . *may* move for the property's return." (emphasis added)); Fed. R. Crim. P. 41(h) ("A defendant *may* move to suppress evidence . . . ." (emphasis added)). Imposing such a prerequisite makes little sense in this context, where Ganias still had the original computer files and did not need the Government's copies to be returned to him. Moreover, we fail to see what purpose a Rule 41(g) motion would have served, given the Government's position that non-responsive files in its possession could not feasibly have been returned or purged anyway.

Because the Government has demonstrated no legal basis for retaining the non-responsive documents, its retention and subsequent search of those documents were unconstitutional. The Fourth Amendment was intended

to prevent the Government from entering individuals' homes and indiscriminately seizing all their papers in the hopes of discovering evidence about previously unknown crimes. *See Entick*, 95 Eng. Rep. at 817-18; *see also Jones*, 132 S. Ct. at 949. Yet this is exactly what the Government claims it may do when it executes a warrant calling for the seizure of particular electronic data relevant to a different crime. Perhaps the "wholesale removal" of intermingled computer records is permissible where off-site sorting is necessary and reasonable, *Tamura*, 694 F.2d at 595-97, but this accommodation does not somehow authorize the Government to retain all non-responsive documents indefinitely, for possible use in future criminal investigations. *See Comprehensive Drug Testing*, 621 F.3d at 1171.

We turn now to the application of the exclusionary rule. As discussed above, suppression is required when (1) there is a widespread seizure of items not covered by the warrant and (2) agents do not act in good faith. *United States v. Shi Yan Liu*, 239 F.3d 138, 141 (2d Cir. 2000). There must also be a weighing of (3) the benefits of deterrence against (4) the costs of suppression. *Herring v. United States*, 555 U.S. 135, 141 (2009).

First, as we set forth above, the Government effected a widespread seizure of files beyond the scope of the warrant -- conduct that resembled an

impermissible general search. *Shi Yan Liu*, 239 F.3d at 141. For almost two-and-a-half years, the Government retained records that were beyond the scope of the 2003 warrant, in violation of Ganias's Fourth Amendment rights.

Second, the agents here did not act in good faith. Government agents act in good faith when they conduct searches in objectively reasonable reliance on binding appellate precedent. *Davis v. United States*, 131 S. Ct. 2419, 2423-24 (2011). It is the Government's burden -- not Ganias's -- to demonstrate the objective reasonableness of the officers' good faith reliance. *United States v. Voustianiouk*, 685 F.3d 206, 215 (2d Cir. 2012). We are not persuaded that the agents in this case reasonably concluded that the 2003 warrant authorized their search of Ganias's personal records and their retention for more than two years. The agents acknowledged, at least initially, that the Government was obliged to "purge[]" the non-responsive data after they completed their search for relevant files. The record also makes clear that Government investigators "viewed the data as the government's property" and intentionally retained Ganias's records for future use. This clearly was not reasonable, and the agents could not have had a good-faith basis to believe the law permitted them to keep the non-responsive files indefinitely.

Third, the benefits of deterrence in this case are great. With the Government's use of forensic mirror images becoming increasingly common, deterring its unconstitutional handling of non-responsive data has grown in importance. The substantial deterrence value in this case is clear when compared to *Davis*, 131 S. Ct. at 2419. In *Davis*, there was no deterrence value because the police officers conducted their search in compliance with appellate precedent at the time. While *Davis*'s appeal was pending in the Eleventh Circuit, the Supreme Court overruled that precedent. There was no cause to deter unlawful Government conduct because the conduct was lawful when it occurred. That is not the situation here. In this case, the Government's handling of Ganas's personal records violated precedent at the time of the search, and relevant Fourth Amendment law has not fundamentally changed since.

Finally, the costs of suppression are minimal here. This is not a case where a dangerous defendant is being set free. See *Herring v. United States*, 555 U.S. 135, 144 (2009) ("The principal cost of applying the [exclusionary] rule is, of course, letting [a] guilty and possibly dangerous defendant[] go free."). Even assuming Ganas committed tax evasion -- a serious matter -- this case does not involve drugs, guns, or contraband. Nor is this a case where police officers

happened upon guns or drugs or other evidence they otherwise could not have found. Rather, early on, the evidence here was readily obtainable by subpoena or search warrant. Moreover, when guns or drugs are suppressed, that evidence is usually irreplaceable. The records here, however, conceivably are available elsewhere as hard copies or can be reconstructed from other records. As made clear by the Government's behavior, the costs of suppression that the Government has asserted are outweighed by the benefits of deterring future misconduct.

Accordingly, we reverse the denial of the motion to suppress and vacate the judgment of conviction.

### *CONCLUSION*

We conclude that the Government violated Ganas's Fourth Amendment rights by seizing and indefinitely retaining non-responsive computer records, and then searching them when it later developed probable cause. Accordingly, Ganas's personal records, seized in the execution of the November 2003 warrant and retained for two-and-a-half years, should have been suppressed. For the reasons stated above, we REVERSE the district court's denial of the motion to suppress, VACATE the judgment of conviction, and REMAND for further proceedings not inconsistent with this opinion.

12-240-cr (en banc)  
*United States v. Ganius*

**UNITED STATES COURT OF APPEALS  
FOR THE SECOND CIRCUIT**

August Term 2015

(Argued: September 30, 2015                      Decided: May 27, 2016)

No. 12-240-cr

---

UNITED STATES OF AMERICA,

*Appellee,*

-v.-

STAVROS M. GANIAS,

*Defendant-Appellant.*

---

Before: KATZMANN, *Chief Circuit Judge*, JACOBS, CABRANES, POOLER, RAGGI, WESLEY, HALL, LIVINGSTON, LYNCH, CHIN, LOHIER, CARNEY, and DRONEY, *Circuit Judges*.

LIVINGSTON and LYNCH, *JJ.*, filed the majority opinion in which KATZMANN, *C.J.*, JACOBS, CABRANES, RAGGI, WESLEY, HALL, CARNEY, and DRONEY, *JJ.*, joined in full, and POOLER and LOHIER, *JJ.*, joined in full as to Parts I and III and in part as to Part II.

LOHIER, *J.*, filed a concurring opinion in which POOLER, *J.*, joined.

CHIN, *J.*, filed a dissenting opinion.

Appeal from the judgment of the United States District Court for the District of Connecticut (Thompson, J.), convicting Defendant-Appellant Stavros Ganiias of two counts of tax evasion, in violation of 26 U.S.C. § 7201. Ganiias argues that the Government retained non-responsive data on mirrored hard drives acquired pursuant to a 2003 search warrant in violation of the Fourth Amendment, and that evidence acquired pursuant to a 2006 search of that data should thus have been suppressed. Because we find that the Government relied in good faith on the 2006 warrant, we need not and do not decide whether the Government violated the Fourth Amendment, and we affirm the judgment of the district court.

AFFIRMED.

SANDRA S. GLOVER (Sarala V. Nagala, Anastasia Enos King, Jonathan N. Francis, Assistant United States Attorneys; Wendy R. Waldron, Senior Counsel, U.S. Dep't of Justice, *on the brief*), *for* Deirdre M. Daly, United States Attorney for the District of Connecticut, *for Appellee United States of America*.

STANLEY A. TWARDY, JR., Day Pitney LLP, Stamford, CT (Daniel E. Wenner, John W. Cerreta, Day Pitney LLP, Hartford, CT, *on the brief*), *for Defendant-Appellant Stavros Ganiias*.

(Counsel for *amici curiae* are listed in Appendix A.)

DEBRA ANN LIVINGSTON and GERARD E. LYNCH, *Circuit Judges*:

Defendant-Appellant Stavros Ganiias appeals from a judgment of the United States District Court for the District of Connecticut (Thompson, J.) convicting him, after a jury trial, of two counts of tax evasion in violation of 26 U.S.C. § 7201. He challenges his conviction on the ground that the Government

violated his Fourth Amendment rights when, after lawfully copying three of his hard drives for off-site review pursuant to a 2003 search warrant, it retained these full forensic copies (or “mirrors”), which included data both responsive and non-responsive to the 2003 warrant, while its investigation continued, and ultimately searched the non-responsive data pursuant to a second warrant in 2006. Ganas contends that the Government had successfully sorted the data on the mirrors responsive to the 2003 warrant from the non-responsive data by January 2005, and that the retention of the mirrors thereafter (and, by extension, the 2006 search, which would not have been possible but for that retention) violated the Fourth Amendment. He argues that evidence obtained in executing the 2006 search warrant should therefore have been suppressed.

We conclude that the Government relied in good faith on the 2006 warrant, and that this reliance was objectively reasonable. Accordingly, we need not decide whether retention of the forensic mirrors violated the Fourth Amendment, and we AFFIRM the judgment of the district court.

## I

### A. Background<sup>1</sup>

In August 2003, agents of the U.S. Army Criminal Investigation Division (“Army CID”) received an anonymous tip that Industrial Property Management (“IPM”), a company providing security for and otherwise maintaining a government-owned property in Stratford, Connecticut, pursuant to an Army contract, had engaged in misconduct in connection with that work. In particular, the informant alleged that IPM, owned by James McCarthy, had billed the Army for work that IPM employees had done for one of McCarthy’s other businesses, American Boiler, Inc. (“AB”), and for construction work performed for IPM’s operations manager at his home residence. The informant told the agents, including Special Agent Michael Conner, that IPM and AB’s financial books were maintained by Stavros Ganiias, a former Internal Revenue Service (“IRS”) agent, who conducted business as Taxes International. On the basis of the informant’s information, as well as extensive additional corroboration, Agent Conner prepared an affidavit seeking three warrants to search the offices of IPM, AB,

---

<sup>1</sup> These facts are drawn from the district court decision denying Ganiias’s motion to suppress and from testimony at the suppression hearing and at Ganiias’s jury trial. With few exceptions noted herein, the facts in this case are not in dispute.

and Taxes International for evidence of criminal activity.<sup>2</sup> Nothing in the record suggests that Ganius himself was suspected of any crimes at that time.

In a warrant dated November 17, 2003, U.S. Magistrate Judge William I. Garfinkel authorized the search of Taxes International. The warrant authorized agents to seize, *inter alia*, “[a]ll books, records, documents, materials, computer hardware and software and computer associated data relating to the business, financial and accounting operations of [IPM] and [AB].” J.A. 433. It further authorized seizure of “[a]ny of the items described [in the warrant] . . . which are stored in the form of magnetic or electronic coding on computer media or on media capable of being read by a computer with the aid of computer-related equipment, including . . . fixed hard disks, or removable hard disk cartridges, software or memory in any form.” *Id.* The warrant also specifically authorized a number of digital search protocols, though it did not state that *only* these

---

<sup>2</sup> Specifically, Agent Conner sought evidence relating to violations of 18 U.S.C. § 287 (making false claims) and § 641 (stealing government property).

protocols were permitted.<sup>3</sup> The warrant authorized seizure of all hardware relevant to the alleged crimes.<sup>4</sup>

---

<sup>3</sup> The warrant specified as follows:

The search procedure of the electronic data contained in computer operating software or memory devices may include the following techniques:

- (a) surveying various file “directories” and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- (b) “opening” or cursorily reading the first few “pages” of such files in order to determine their precise contents;
- (c) “scanning” storage areas to discover and possibly recover recently deleted files;
- (d) “scanning” storage areas for deliberately hidden files; or
- (e) performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation.

J.A. 433-34.

<sup>4</sup> In his attached affidavit, Agent Conner offered three reasons why it was necessary for the agents to take entire hard drives off-site for subsequent search rather than search the hard drives on-site: First, he stated that computer searches had to be conducted by computer forensics experts, who “us[ed] . . . investigative techniques” to both “protect the integrity of the evidence . . . [and] detect hidden, disguised, erased, compressed, password protected, or encrypted files.” J.A. 448-49. Because of “[t]he vast array” of software and hardware available, it would not always be possible “to know before a search which expert is qualified to analyze the [particular] system and its data.” J.A. 450. Thus, the appropriate experts could not be expected, in all cases, to accompany agents to the relevant site to be searched. Second, Agent Conner affirmed that such searches often must occur in “a laboratory or other controlled environment” given the sensitivity of the digital storage media. J.A. 449-50. And third, he stated that “[t]he search process can take weeks or months, depending on the particulars of the hard drive to be searched.” J.A. 449. The district court found, in denying Ganas’s

On November 19, 2003, Army CID agents executed the search warrants. Because the warrants authorized the seizure of computer hardware and software, in addition to paper documents, Agent Conner sought the help, in executing the warrants, of agents from the Army CID's Computer Crimes Investigation Unit ("CCIU"), a unit with specialized expertise in digital forensics and imaging. At Ganias's office, the CCIU agents — and in particular Special Agent David Shaver — located three computers. Rather than take the physical hard drives, which would have significantly impaired Ganias's ability to conduct his business, Agent Shaver created mirror images: exact copies of all of the data stored thereon, down to the bit.<sup>5</sup> Ganias was present at his office during the creation of the mirrors, spoke with the agents, and was aware that mirrored

---

motion to suppress, that, as a result of technological limitations in 2003 and the complexities of searching digital data, "[a] full [on-site] search would have taken months to complete." *United States v. Ganias*, No. 3:08CR00224 (AWT), 2011 WL 2532396, at \*2 (D. Conn. June 24, 2011).

<sup>5</sup> Hard drives are storage media comprising numerous bits — units of data that may be expressed as ones or zeros. Mirroring involves using a commercially available digital software (in the present case, though not always, EnCase) to obtain a perfect, forensic replica of the sequence of ones and zeros written onto the original hard drive. During the mirroring, EnCase acquires metadata about the mirroring process, writing an unalterable record of who creates the copy and when the copy is created. It also assigns the mirror a "hash value" — a unique code that can be used to verify whether, upon subsequent examination of the mirror at any later date, even a single one or zero has been altered from the original reproduction.

copies of his three hard drives had been created and taken off-site.<sup>6</sup> There is no dispute that the forensic mirrors taken from Ganias's office contained all of the computerized data maintained by Ganias's business, including not only material related to IPM or AB, but also Ganias's own personal financial records, and the records of "many other" accounting clients of Ganias: businesses of various sorts having no connection to the Government's criminal investigation.<sup>7</sup> J.A. 464, ¶ 14.

---

<sup>6</sup> Testifying at the suppression hearing, Agent Conner explained that the decision to take mirrors, rather than the hard drives themselves, reflected a desire to mitigate the burden on Ganias and his business. *See* J.A. 140-41. The district court credited this testimony, concluding that the agents "used a means less intrusive to the individual whose possessions were seized than other means they were authorized to use." *Ganias*, 2011 WL 2532396, at \*8. The district court, further, explicitly found that the 2003 warrant authorized the Government to take these mirrors, *id.* at \*10, a position Ganias has not challenged on appeal, and that runs directly counter to the dissent's seeming suggestions that the Government somehow acted improperly when it mirrored Ganias's hard drives or that this initial seizure went beyond the scope of the 2003 warrant, *see, e.g.*, Dissent at 3 (noting that "although the Government had a warrant for documents relating to only two of defendant-appellant Stavros Ganias's accounting clients, it seized *all* the data from three of his computers"); *id.* at 40 (stating that "the Government . . . entered Ganias's premises with a warrant to seize certain papers and indiscriminately seized — and *retained* — all papers instead").

<sup>7</sup> Ganias claimed before the district court that when he expressed some concern about the scope of the data being seized, an agent assured him that the agents were only looking for files related to AB and IPM, and that irrelevant files "would be purged once they completed their search" for such files. J.A. 428. The district court made no finding to this effect, however. It is undisputed, moreover, that Ganias became aware in February 2006 that the Government retained the mirrors and sought to search them in connection with Ganias's own tax reporting. At no time thereafter did Ganias seek return of the mirrors pursuant to Federal Rule of Criminal Procedure 41(g) or otherwise contact a case agent to seek their return or destruction.

The next day, Agent Shaver consolidated the eleven mirrored hard drives from all three searches (including the three from Ganias's office) onto a single external hard drive which he provided to Agent Conner. Agent Conner, in turn, provided this hard drive to the evidence custodian of the Army CID, who stored it at Fort Devens, Massachusetts. There the consolidated drive remained, unaltered and untouched, throughout the events relevant to this case. Around the same time, Agent Shaver created two additional copies of the mirrored drives on two sets of nineteen DVDs. After providing these DVD sets to Agent Conner, Agent Shaver then purged the external hard drives onto which he had originally written the mirrors. At this point, a week after the search, three complete copies of the mirrors of Ganias's hard drives existed: an untouched copy stowed away in an evidence locker and two copies available for forensic analysis.<sup>8</sup>

Though internal protocols required that specialized digital forensic analysts search the mirrored hard drives, the paper files were not subject to such limitations. Thus, shortly after the November 19 seizure, the Army CID agents

---

<sup>8</sup> These copies were identical digital replicas of Ganias's hard drives as mirrored on November 19, 2003. Notably, the original hard drives in Ganias's computers had already been significantly altered since the Government mirrored them. Ganias explains in his brief before this Court that "[t]wo days after the execution of the November 2003 warrant, [he] reviewed his personal QuickBooks file and . . . *corrected over 90 errors in earlier journal entries.*" Appellant Br. at 15 n.7 (emphasis added).

began to analyze the non-digital files seized pursuant to the warrant. These files suggested that IPM had made payments to a third company whose owner, according to the Connecticut Department of Labor, was a full-time employee of an insurance company who received no wages from any source other than that insurance company. This and other red flags spurred Agent Conner to contact the Criminal Investigation Division of the IRS, which subsequently joined the investigation.

In early February 2004, as he and his fellow agents continued to follow leads from the paper files, Agent Conner sent one of the two DVD sets containing the forensic mirrors to the Army Criminal Investigation Laboratory ("ACIL") in Forest Park, Georgia, accompanied by a copy of one of the three search warrants. In early June, the ACIL assigned Gregory Norman, a digital evidence examiner, to perform a forensic analysis. Around the same time, Special Agent Michelle Chowaniec, who replaced Agent Conner as the primary case agent for the Army CID in late March, provided the second set of DVDs to the IRS agent assigned to the case, Special Agent Paul Holowczyk. Agent Holowczyk in turn, passed it on, by way of intermediaries, to Special Agent Vita Paukstelis, a computer investigative specialist. By the end of June 2004,

computer experts for the Army CID and the IRS — Norman and Agent Paukstelis, respectively — had received copies of the digital evidence (which, as the district court found, were “encoded so that only agents with forensic software not directly available to the case agents could view [them],” *Ganias*, 2011 WL 2532396, at \*7), and forensic examination began.

Norman commenced his analysis in late June by loading the eleven mirrored drives into EnCase — the same software with which Agent Shaver initially created the mirrors — so that he could search the data thereon. After looking at the search warrants, he created a number of keywords, with which he searched for potentially relevant data. Initially, the search returned far too many results for practicable review (more than 17,000 hits); thus, Norman requested new keywords from Agent Chowaniec. On the basis of these new keywords, he was able to narrow his search and ultimately identify several files he thought might be of interest to the investigation, all of which he put on a single CD.<sup>9</sup> Some of these files he was able personally to examine, to determine whether they were responsive to the warrant; a few (including the QuickBooks file labeled

---

<sup>9</sup> The rest of the data remained on the DVDs, where agents would not be able to access it without specific forensic software. *See Ganias*, 2011 WL 2532396, at \*7.

"Steve\_ga.qbw," which was ultimately searched pursuant to the 2006 warrant, J.A. 467) Norman could not open without a specific software edition of QuickBooks to which he did not have immediate access. However, as these files (like the others) contained keywords that were taken from the narrower list and generated on the basis of the warrant, Norman included the QuickBooks files in the CD he ultimately sent to Agent Chowaniec along with a report.<sup>10</sup> On July 23, 2004, Chowaniec received this CD. Norman, in turn, returned the nineteen DVDs to Army CID's evidence custodian in Boston for safekeeping.

Norman's counterpart in the IRS, Agent Paukstelis — who, in addition to receiving the search warrant with her set of DVDs, also received a list of companies, addresses, and key individuals relating to the investigation, along with "a handwritten notation next to the name 'Taxes International' that stated '(return preparer) do not search,'" *Ganias*, 2011 WL 2532396, at \*3 — conducted her analysis over a period of about four months. Because she worked for the IRS, she limited her search to the three mirrored drives from Taxes International. Though Agent Paukstelis used ILook, a different software program, to review the mirrored hard drives, she too could not open QuickBooks files without the

---

<sup>10</sup> Norman describes the storage device he sent to Chowaniec as a "DVD," J.A. 218; the district court described it as a "CD," *Ganias*, 2011 WL 2532396, at \*4. The distinction is immaterial.

relevant proprietary software. Still, though she could not open these files, she believed, based on the information to which she had access, that they were within the scope of the warrant; thus, in October 2004, she copied this data, in concert with other responsive data, onto a CD, three copies of which she sent to Agent Holowczyk and Special Agent Amy Hosney, also with the IRS. In light of the note she had received with her DVD set as well as the list of relevant entities, Agent Paukstelis avoided, to the degree she could, searching any files of Taxes International that did not appear to be directly relevant to that list. On November 30, 2004, Paukstelis also provided a “restoration” of the mirrors of the Taxes International hard drives to Special Agent George Francischelli, an IRS computer specialist assigned to the case.<sup>11</sup>

Agents Chowanec and Conner, after receiving Norman’s CD and report in late July, conducted initial reviews of the data. Like Norman and Agent Paukstelis, however, they could not open the QuickBooks files. At the same time, the agents were busy, in the words of Agent Chowanec, “tracking down other leads[,]... [issuing] grand jury subpoenas, ... doing interviews of

---

<sup>11</sup> A “restoration” is a software interface that enables a user (potentially a jury) to view data on a mirror as such data would have appeared to a person accessing the data on the original storage device at the time the mirror was created. *Ganias*, 2011 WL 2532396, at \*4.

subcontractors and identifying subcontractors from the papers that [the agents had] received from the search warrants.” J.A. 294-95. In October, Agents Hosney and Chowaniec attempted, together, to review the QuickBooks files, but again lacked the relevant software to do so. Finally, in November 2004, Agent Chowaniec, having acquired the appropriate software, opened two IPM QuickBooks files on her office computer, and then in December, Agents Hosney and Chowaniec, using the restoration provided by Agent Paukstelis, looked at additional IPM QuickBooks files. Though they had the entirety of the mirrored data before them (the only time throughout the investigation that the case agents had direct access to a software interface permitting them to view essentially all of the data stored on the mirrors), they carefully limited their search: Agent Hosney testified that they “only looked at the QuickBooks files for Industrial Property Management and American Boiler...[b]ecause those were the only two companies named in the search warrant attachment.” J.A. 340. They did, however, observe that other files existed — both on the CD Norman had provided and on the restoration — in particular, the files Agent Hosney ultimately searched in 2006.

Ganias contends that there is no dispute that by this point, the agents had finished “identifying and segregating the files within the November 2003 warrant’s scope.” Appellant Reply Br. at 5. In actuality, the record is unclear as to whether the forensic examination of the mirrored computers pursuant to the initial search warrant had indeed concluded as a forward-looking matter, rather than from the perspective of hindsight.<sup>12</sup> The district court did not find any facts decisive to this question. It is, further, undisputed that the investigation into McCarthy, IPM, and AB was ongoing at this time, and that this investigation would culminate in an indictment of McCarthy in 2008 secured in large part through reliance on evidence responsive to the 2003 warrant and located on the mirrored copies of Ganias’s hard drives. *See* Indictment, *United States v. McCarthy*,

---

<sup>12</sup> At the suppression hearing, Agent Chowaniec testified, in response to the question whether “as of mid-December, [her] forensic analysis was completed”: “That’s correct, of the computers.” J.A. 322. But when asked later, “[D]id you know [in December 2004] you wouldn’t need to look at any information that had been provided by Greg Norman on that CD anymore in the course of this investigation,” Agent Chowaniec responded, “No,” and when further asked, “Did you know you wouldn’t require further analysis by Greg Norman or any other examiner at the Army lab in Georgia after December of 2004,” Agent Chowaniec again responded, “No.” J.A. 324. Agent Conner similarly answered with uncertainty when asked a related question. *See* J.A. 145 (“I didn’t know the entire universe of information that was contained within the DVDs that were sent to [Norman] for analysis. I knew only what he sent back to me saying this is what I found off your keyword search.”). The dissent disputes our conclusion that the record was unclear on this point, arguing, through citation to Agent Chowaniec’s testimony, that “the record . . . shows otherwise.” Dissent at 19. The district court found no facts on this issue, and the record, as demonstrated above, is indeed unclear.

No. 3:08cr224 (EBB) (D. Conn. Oct. 31, 2008), ECF No. 1. When asked why, at this time or any time later, Agent Conner did not return or destroy the data stored on the mirrors that did not appear directly to relate to the crimes alleged in the warrant, Agent Conner explained that “[the] investigation was still . . . open” and that, generally, items would be “released back to the owner” once an investigation was closed. J.A. 123. He further noted that the Army CID “would not routinely go into DVDs to delete data, as we’re altering the original data that was seized.” J.A. 122.<sup>13</sup>

Over the next year, the agents continued to investigate IPM and AB. Analysis of the paper files taken pursuant to the November 2003 search warrant

---

<sup>13</sup> Agent Conner’s explanation for why the Government did not, as a matter of policy in this or other cases, delete mirrored drives or otherwise require segregation or deletion of non-responsive data, is not a model of clarity: in addition to citing concerns of evidentiary integrity and suggesting a policy of non-deletion or return prior to the end of an investigation, he noted that “you never know what data you may need in the future,” J.A. 122, and at one point referred to the DVDs as “the government’s property, not Mr. Ganas’[s] property,” J.A. 146. The dissent seizes on this single sentence during Agent Conner’s cross-examination as the smoking gun of the Government’s bad faith, citing it on no fewer than four occasions. *See* Dissent at 3, 8, 33, 37. The district court, however, did not find facts explicating Agent Conner’s testimony or placing it within the context of the explanations that he and other agents offered for retention of the mirrors. The court did note in its legal analysis that “[a] copy of the evidence was preserved in the form in which it was taken.” *Ganas*, 2011 WL 2532396, at \*8. Further, the Government on appeal provides numerous rationales — many echoing those articulated by Agent Conner *throughout* his testimony — for why retention of a forensic mirror may be necessary during the pendency of an investigation, none of which amounts to the argument that the mirror is simply “government[] property.”

revealed potential errors in AB's tax returns that seemed to omit income reflected in checks deposited into IPM's account. Aware that Ganias had prepared these tax returns and deposited the majority of these checks, Agent Hosney came to suspect that Ganias was engaged in tax-related crimes.<sup>14</sup> She did not, however, return to the restoration or otherwise open any of Ganias's digital financial documents or files associated with Taxes International.<sup>15</sup> Instead, Agent Hosney subpoenaed Ganias's bank records from 1999 to 2003 and accessed his income

---

<sup>14</sup> The dissent suggests that "[w]hat began nearly thirteen years ago as an investigation by the Army into two of Ganias's business clients *somehow* evolved into an unrelated investigation by the IRS into Ganias's personal affairs, largely because" the Government retained the mirrored copies of Ganias's hard drives. Dissent at 40 (emphasis added). In fact, Agent Hosney's affidavit in support of the 2006 warrant explains that the Government suspected Ganias of underreporting his income because of evidence that Ganias had assisted McCarthy in underreporting income from *McCarthy's* companies — evidence which led to an indictment of *both* McCarthy and Ganias for conspiracy to commit tax fraud. Further, when Agent Hosney developed this suspicion — which was hardly "unrelated" to the initial investigation — she did not turn to the mirrors, but instead engaged in old-fashioned investigatory work, "examin[ing Ganias's tax returns] more closely to determine if his own income was underreported." J.A. 465, ¶ 18. She then reviewed deposits in his bank account, cross-referenced bank records and tax returns, and finally presented this evidence in a proffer session to Ganias — all without once looking at any non-responsive information on the mirrors. Only after she had acquired independent probable cause — and only after extensive evidence suggested Ganias may have committed a crime — did Agent Hosney seek a second warrant to search the mirrors. It is, in short, no mystery how the investigation of McCarthy, IPM, and AB came to include Ganias, and, further, an inaccurate statement of the record to suggest that this "evolution" had anything to do with the retention of the mirrors.

<sup>15</sup> Agent Hosney explained in her testimony: "[W]e couldn't look at that file because it wasn't — Steve Ganias and Taxes International were not listed on the original Attachment B, items to be seized." J.A. 348.

tax returns for the same period. On July 28, 2005, the IRS — believing Ganas to be involved both personally and as an accomplice or co-conspirator in tax evasion — officially expanded the investigation to include him.

On February 14, 2006, Ganas, accompanied by his lawyer, met in a proffer session with Agent Hosney and others involved in the investigation.<sup>16</sup> That day or shortly thereafter, Agent Hosney asked Ganas for consent to access his personal QuickBooks files and those of his business, Taxes International — data Agent Hosney knew to be present on the forensic mirrors but which she had not accessed. When, by April 24, 2006 (two and a half months later), Ganas had failed to respond (either by consenting, objecting, or filing a motion under Federal Rule of Criminal Procedure 41(g) for return of seized property), Agent Hosney sought a search warrant to search the mirrored drives again.<sup>17</sup> In her search warrant affidavit, Agent Hosney pointed to bank records, income tax forms, and additional evidence to demonstrate that she had probable cause to

---

<sup>16</sup> According to Agent Hosney, in that proffer session Ganas claimed “that he failed to record income from his own business [to his QuickBook files] as a result of a computer flaw in the QuickBooks software . . . [but that,] . . . although he attempted to duplicate the software error, he was unable to do so.” J.A. 467, ¶ 28. Agent Hosney contacted Intuit, Inc., which released QuickBooks, to determine whether such an error might have affected, generally, the pertinent version of the software, and was told that the company was aware of no such “widespread malfunction.” J.A. 469, ¶ 35.

<sup>17</sup> U.S. Magistrate Judge William I. Garfinkel, who had authorized the 2003 warrant, authorized this 2006 warrant as well. J.A. 430, 454.

believe that Ganas had violated 26 U.S.C. § 7201 (by committing tax evasion) and § 7206(1) (by making false declarations).<sup>18</sup> She further noted that the items to be searched were “mirror images of computers seized on November 19, 2003 from the offices of Taxes International,” J.A. 461, ¶ 7; that information material to the initial investigation had been located on these mirrors and that, “[d]uring th[at] investigation,” such information had been “analyzed in detail,” J.A. 464, ¶ 15; that Ganas was not, at the time of the initial seizure, under investigation, J.A. 461, ¶ 3 (“On July 28, 2005, the Government’s investigation was expanded to include an examination of whether Ganas, McCarthy’s accountant and former IRS Revenue Agent, violated the federal tax laws.”); and thus that, though Agent Hosney believed that the second mirrored drive, called TaxInt\_2, was “the primary computer for Taxes International,” J.A. 463, ¶ 13, she could not search Ganas’s personal or business files as “[p]ursuant to the 2003 search warrant, only files for [AB] and IPM could be viewed,” J.A. 464, ¶ 14. The magistrate judge issued the warrant, Agent Hosney searched the referenced data, and ultimately the Government indicted Ganas for tax evasion.

---

<sup>18</sup> Ganas did not contest before the district court, and does not contest on appeal, that this evidence — none of which was acquired through search of non-responsive data on the mirrors — created sufficient probable cause for the 2006 warrant.

## B. Procedural History

In February 2010, Ganas moved to suppress the evidence Agent Hosney acquired pursuant to the 2006 warrant. After a two-day hearing, the district court denied the motion on April 14, 2010, and issued a written decision on June 24, 2011. In that decision, the district court found, *inter alia*, that the forensic examination of the mirrored drives “was conducted within the limitations imposed by the [2003] warrant” and that “[a] copy of the evidence was preserved in the form in which it was taken.” *Ganas*, 2011 WL 2532396, at \*8. Judge Thompson observed that Ganas “never moved for destruction or return of the data, which could have led to the seized pertinent data being preserved by other means.” *Id.* The district court concluded that the Government’s retention of the mirrored drives — and thus its subsequent search of those drives pursuant to a warrant — did not violate the Fourth Amendment. Having found no Fourth Amendment violation, the district court did not reach the question of good faith. *Id.* at \*9.

At trial, the Government introduced information in Ganas’s QuickBooks files as evidence against him, in particular highlighting the fact that payments made to him by clients such as IPM were characterized as “owner’s

contributions,” which prevented QuickBooks from recognizing them as income.<sup>19</sup> On the basis of this and other evidence, the jury convicted Ganas of two counts of tax evasion, and the district court sentenced him to two terms of 24 months’ incarceration, to be served concurrently.

Ganas appealed. On review of his conviction, a panel of this Court concluded, unanimously, that the Government had violated the Fourth Amendment; in a divided decision, the panel then ordered suppression of the evidence obtained in executing the 2006 warrant and vacated the jury verdict. We subsequently ordered this rehearing *en banc* in regards to, first, the existence of a Fourth Amendment violation and, second, the appropriateness of suppression.<sup>20</sup>

---

<sup>19</sup> Many of these entries existed *only* on the QuickBooks files that the Government had accessed on the mirrors, as a result of Ganas’s amendments to the entries on his hard drives days after the execution of the 2003 warrant. At trial, Ganas testified that his characterization of the payments as “owner’s contributions” was simply a good faith mistake, and not evidence of intent to commit tax evasion, a claim that the Government labeled implausible in light of Ganas’s extensive experience as an IRS agent and accountant.

<sup>20</sup> Specifically, we asked the parties to brief the following two issues:

- (1) Whether the Fourth Amendment was violated when, pursuant to a warrant, the government seized and cloned three computer hard drives containing both responsive and non-responsive files, retained the cloned hard drives for some two-and-a-half years, and then searched the non-responsive files pursuant to a subsequently issued warrant; and

## II

“On appeal from a district court’s ruling on a motion to suppress evidence, ‘we review legal conclusions de novo and findings of fact for clear error.’” *United States v. Bershchansky*, 788 F.3d 102, 108 (2d Cir. 2015) (quoting *United States v. Freeman*, 735 F.3d 92, 95 (2d Cir. 2013)). We may uphold the validity of a judgment “on any ground that finds support in the record.” *Headley v. Tilghman*, 53 F.3d 472, 476 (2d Cir. 1995).

The district court concluded that the conduct of the agents in this case comported fully with the Fourth Amendment, and thus did not reach the question whether they also acted in good faith. Because we conclude that the agents acted in good faith, we need not decide whether a Fourth Amendment violation occurred. We thus affirm the district court on an alternate ground. Nevertheless, though we offer no opinion on the existence of a Fourth Amendment violation in this case, we make some observations bearing on the reasonableness of the agents’ actions, both to illustrate the complexity of the questions in this significant Fourth Amendment context and to highlight the

---

(2) Considering all relevant factors, whether the government agents in this case acted reasonably and in good faith such that the files obtained from the cloned hard drives should not be suppressed.

*United States v. Ganius*, 791 F.3d 290 (2d Cir. 2015) (mem.).

importance of careful consideration of the technological contours of digital search and seizure for future cases.

“The touchstone of the Fourth Amendment is reasonableness . . . .” *United States v. Miller*, 430 F.3d 93, 97 (2d Cir. 2005) (alteration omitted) (quoting *United States v. Knights*, 534 U.S. 112, 118 (2001)). As relevant here, “searches pursuant to a warrant will rarely require any deep inquiry into reasonableness.” *United States v. Leon*, 468 U.S. 897, 922 (1984) (alteration omitted) (quoting *Illinois v. Gates*, 462 U.S. 213, 267 (1983) (White, J., concurring in judgment)). Nevertheless, both the scope of a seizure permitted by a warrant,<sup>21</sup> and the reasonableness of

---

<sup>21</sup> Specifically, courts have long recognized that a prohibition on “general warrants” — warrants completely lacking in particularity — was a central impetus for the ratification of the Fourth Amendment. *See, e.g., Riley v. California*, 134 S. Ct. 2473, 2494 (2014) (noting, in the context of evaluating the reasonableness of a warrantless search of a cell phone, that “[o]ur cases have recognized that the Fourth Amendment was the founding generation’s response to the reviled ‘general warrants’ and ‘writs of assistance’ of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity” and that “opposition to such searches was in fact one of the driving forces behind the Revolution itself”); *Marshall v. Barlow’s, Inc.*, 436 U.S. 307, 311 (1978) (noting, in the context of evaluating the reasonableness of warrantless inspections of business premises, that “[t]he particular offensiveness” of general warrants “was acutely felt by the merchants and businessmen whose premises and products were inspected” under them); *Stanford v. Texas*, 379 U.S. 476, 486 (1965) (“[T]he Fourth . . . Amendment[] guarantee[s] . . . that no official . . . shall ransack [a person’s] home and seize his books and papers under the unbridled authority of a general warrant . . . .”); *United States v. Galpin*, 720 F.3d 436, 445 (2d Cir. 2013) (“The chief evil that prompted the framing and adoption of the Fourth Amendment was the ‘indiscriminate searches and seizures’ conducted by the British

government conduct in executing a valid warrant,<sup>22</sup> can present Fourth Amendment issues. Ganas thus argues that the Government violated the Fourth Amendment in this case, notwithstanding the two warrants that issued, by retaining complete forensic copies of his three hard drives during the pendency of its investigation.

According to Ganas, when law enforcement officers execute a warrant for a hard drive or forensic mirror that contains data that, as here, cannot feasibly be

---

‘under the authority of “general warrants.”’ (quoting *Payton v. New York*, 445 U.S. 573, 583 (1980))).

We agree with the dissent that “the precedents are absolutely clear that general warrants are unconstitutional.” Dissent at 30. To the degree that the dissent would go further, however, and find it “absolutely clear” to a reasonable government agent in 2005 that the retention of a lawfully acquired mirror during the pendency of an investigation and the subsequent search of data on that mirror pursuant to a second warrant would implicate the ban on general warrants, we respectfully disagree.

<sup>22</sup> See, e.g., *L.A. Cty. v. Rettele*, 550 U.S. 609, 614-16 (2007) (applying the reasonableness standard to evaluate whether police officers’ manner of executing a valid warrant violated the Fourth Amendment); *Wilson v. Layne*, 526 U.S. 603, 611 (1999) (“[T]he Fourth Amendment does require that police actions in execution of a warrant be related to the objectives of the authorized intrusion . . . .”); *Dalia v. United States*, 441 U.S. 238, 258 (1979) (“[T]he manner in which a warrant is executed is subject to later judicial review as to its reasonableness.”); *Terebesi v. Torres*, 764 F.3d 217, 235 (2d Cir. 2014) (“[T]he method used to execute a search warrant . . . [is] as a matter of clearly established constitutional law, subject to Fourth Amendment protections . . . .”), *cert. denied sub nom. Torres v. Terebesi*, 135 S. Ct. 1842 (2015) (mem.); *Lauro v. Charles*, 219 F.3d 202, 209 (2d Cir. 2000) (“[T]he Fourth Amendment’s proscription of unreasonable searches and seizures ‘not only . . . prevent[s] searches and seizures that would be unreasonable if conducted at all, but also . . . ensure[s] reasonableness in the manner and scope of searches and seizures that are carried out.’” (all but first alteration in original) (quoting *Ayeni v. Mottola*, 35 F.3d 680, 684 (2d Cir. 1994))).

sorted into responsive and non-responsive categories on-site, “the Fourth Amendment demands, at the very least, that the officers expeditiously complete their off-site search and then promptly return (or destroy) files outside the warrant’s scope.”<sup>23</sup> Appellant Br. at 18. Arguing that a culling process took place here and that it had concluded by, at the latest, January 2005, Ganas faults the Government for retaining the mirrored drives — including storing one

---

<sup>23</sup> On appeal, Ganas does not question the scope or validity of the 2003 warrant. The district court found that the 2003 warrant authorized the Government to mirror Ganas’s hard drives for off-site review, *Ganas*, 2011 WL 2532396, at \*10; that the warrant, though authorizing such seizure, was sufficiently particularized and not a “general warrant,” *id.*; that, absent mirroring for off-site review, on-site review would have taken months, *id.* at \*2; and that mirroring thus minimized any intrusion on Ganas’s business, *id.* at \*8; *cf.* Fed. R. Crim. P. 41(e)(2)(B) (which, as amended in 2009, permits a warrant to “authorize the seizure of electronic storage media or the seizure or copying of electronically stored information,” and notes that “[u]nless otherwise specified, the warrant authorizes a later review of the media or information consistent with the warrant”); Fed. R. Crim. P. 41(e)(2)(B) advisory committee’s note to 2009 amendments (explaining that, because “[c]omputers and other electronic storage media commonly contain such large amounts of information that it is often impractical for law enforcement to review all of the information during execution of the warrant at the search location[, t]his rule acknowledges the need for a two-step process: officers may seize or copy the entire storage medium and review it later to determine what electronically stored information falls within the scope of the warrant”). Ganas does not contest these conclusions on appeal but contends, instead, that considerations *underlying* the prohibition on general warrants may require that, if the government lawfully mirrors an entire hard drive containing non-responsive as well as responsive information for off-site review, it may not then retain the mirror throughout the pendency of its investigation.

forensic copy in an evidence locker for safekeeping.<sup>24</sup> It was this retention, he argues, that constituted the Fourth Amendment violation — a violation that, in turn, made the 2006 search of the data itself unconstitutional as, but for this retention, the search could never have occurred.

To support this argument, Ganas relies principally on *United States v. Tamura*, 694 F.2d 591 (9th Cir. 1982), a Ninth Circuit case involving the search and seizure of physical records. In *Tamura* (unlike the present case, in which a warrant specifically authorized the agents to seize hard drives and to search them off-site) officers armed only with a warrant authorizing them to seize specific “records” instead seized numerous boxes of printouts, file drawers, and cancelled checks for off-site search and sorting. *Id.* at 594-95. After the officers had clearly sorted the responsive paper documents from the non-responsive ones, they refused — despite request — to return the non-responsive paper files. *Id.* at 596-97. The Ninth Circuit concluded that both the unauthorized seizure of voluminous material not specified in the warrant and the retention of the seized

---

<sup>24</sup> As already noted, the district court made no finding as to when or whether forensic examination of the mirrors pursuant to the 2003 warrant was completed.

documents violated the Fourth Amendment.<sup>25</sup> *Id.* at 595, 597; *see also Andresen v. Maryland*, 427 U.S. 463, 482 n.11 (1976) (“[W]e observe that to the extent [seized] papers were not within the scope of the warrants or were otherwise improperly seized, the State was correct in returning them voluntarily and the trial judge was correct in suppressing others. . . . In searches for papers, it is certain that some innocuous documents will be examined, at least cursorily, in order to determine whether they are, in fact, among those papers authorized to be seized. . . . [R]esponsible officials [conducting such searches], including judicial officials, must take care to assure that they are conducted in a manner that minimizes unwarranted intrusions upon privacy.”); *cf. United States v. Matias*, 836 F.2d 744, 747 (2d Cir. 1988) (“[W]hen items outside the scope of a valid warrant are seized, the normal remedy is suppression and return of those items . . .”).

Because we resolve this case on good faith grounds, we need not decide the relevance, if any, of *Tamura* (or, more broadly, the validity of Ganias’s Fourth Amendment claim). We note, however, that there are reasons to doubt whether *Tamura* (to the extent we would indeed follow it) answers the questions before us. First, on its facts, *Tamura* is distinguishable from this case, insofar as the

---

<sup>25</sup> The Ninth Circuit declined to reverse the defendant’s conviction, as no improperly seized document was admitted at trial, and as blanket suppression was not warranted. *See Tamura*, 694 F.2d at 597.

officers there seized for off-site review records that the warrant did not authorize them to seize,<sup>26</sup> and retained those records even after their return was requested. Here, in contrast, the warrant authorized the seizure of the hard drives, not merely particular records, and Ganas did not request return or destruction of the mirrors (even after he was indisputably alerted to the Government's continued retention of them) by, for instance, filing a motion for such return pursuant to Federal Rule of Criminal Procedure 41(g). Second, and more broadly, even if the facts of *Tamura* were otherwise on point, Ganas's invocation of *Tamura's* reasoning rests on an analogy between paper files intermingled in a file cabinet and digital data on a hard drive. Though we do not take any position on the ultimate disposition of the constitutional questions herein, we nevertheless pause to address the appropriateness of this analogy, which is often invoked (including by the dissent) and bears examination.

The central premise of Ganas's reliance on *Tamura* is that the search of a digital storage medium is analogous to the search of a file cabinet. The analogy has some force, particularly as seen from the perspective of the affected

---

<sup>26</sup> The fact that the officers in *Tamura* lacked a warrant for the initial seizure was not incidental to the decision: the *Tamura* court explicitly found that it was the lack of a warrant that made the initial seizure — even if otherwise understandable in light of the voluminous material to be reviewed — a violation of the Fourth Amendment. *See* 694 F.2d at 596.

computer user. Computer users — or at least, average users (in contrast to, say, digital forensics experts) — typically experience computers as filing cabinets, as that is precisely how user interfaces are designed to be perceived by such users.<sup>27</sup> Given that the file cabinet analogy (at least largely) thus captures an average person’s subjective experience with a computer interface, the analogy may shed light on a user’s subjective expectations of privacy regarding data maintained on a digital storage device. Because we experience digital files as discrete items, and because we navigate through a computer as through a virtual storage space, we may expect the law similarly to treat data on a storage device as comprised of distinct, severable files, even if, in fact, “[s]torage media do not naturally divide into parts.” Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 Berkeley J. Crim. L. 112, 131 (2011). In this case, for example, a person in

---

<sup>27</sup> See Daniel B. Garrie & Francis M. Allegra, Fed. Judicial Ctr., *Understanding Software, the Internet, Mobile Computing, and the Cloud: A Guide for Judges* 8-14 (2015) (contrasting “operating systems . . . [which] hide the hardware resources behind abstractions to provide an environment that is more user-friendly,” *id.* at 13, with machine language, assembly language, high-level languages, data structures, and algorithms); Josh Goldfoot, *The Physical Computer and the Fourth Amendment*, 16 Berkeley J. Crim. L. 112, 117 (2011) (contrasting two perspectives on digital storage media — the “internal perspective,” or how “the user experiences [such media,] as parcels of information, grouped into files, or even into smaller units such as spreadsheet rows” and the “external perspective,” or how the actual computer functions, in which “files are not . . . ‘things’ at all,” but “groupings of data . . . inseparably tied to the storage medium,” created by the computer by manipulating “chunks of physical matter [such as regions on a hard drive] whose state is altered to record information”).

Ganias's situation could well understand the "files" on his hard drives containing information relating to IPM and AB as separate from the "files" containing his personal financial information and that of other clients. Indeed, the very fact that the Government sought additional search authorization via the 2006 warrant when it established probable cause to search Ganias's personal files indicates that the Government too understood — and credited — this distinction.

That said, though it may have some relevance to our inquiry, the file cabinet analogy is only that — an analogy, and an imperfect one. Cf. James Boyle, *The Public Domain* 107 (2008) ("Analogies are only bad when they ignore the key difference between the two things being analyzed."). Though to a user a hard drive may seem like a file cabinet, a digital forensics expert reasonably perceives the hard drive simply as a coherent physical storage medium for digital data — data that is interspersed *throughout* the medium, which itself must be maintained and accessed with care, lest this data be altered or destroyed.<sup>28</sup> See

---

<sup>28</sup> See Eoghan Casey, *Digital Evidence and Computer Crime* 472, 474-96 (3d ed. 2011) (highlighting the fact that forensic examination of storage media can create tiny alterations, which necessitates care on the part of examiners in acquiring, searching, and preserving that data); *id.* at 477-78 (describing the importance of protecting digital storage media from "dirt, fluids, humidity, impact, excessive heat and cold, strong magnetic fields, and static electricity"); Michael W. Graves, *Digital Archaeology: The Art and Science of Digital Forensics* 95 (2014) ("Computer data is extremely volatile and easily deleted, and can be destroyed, either intentionally or accidentally, with a few mouse

Goldfoot, *supra*, at 114 (arguing digital storage media are physical objects like “drugs, blood, or clothing”); Wayne Jekot, *Computer Forensics, Search Strategies, and the Particularity Requirement*, 7 U. Pitt. J. Tech. L. & Pol’y, art. 5, at 1, 30 (2007) (“[A] computer does not simply hold data, it is *composed* of data.”). Even the most conventional “files” – word documents and spreadsheets such as those the Government searched in this case – are not maintained, like files in a file cabinet, in discrete physical locations separate and distinct from other files. They are in fact “fragmented” on a storage device, potentially across physical locations. Jekot, *supra*, at 13. “Because of the manner in which data is written to the hard drive, rarely will one file be stored intact in one place on a hard drive,” *id.*; so-called “files” are stored in multiple locations and in multiple forms, *see*

---

clicks.”); Bill Nelson et al., *Guide to Computer Forensics and Investigations* 160 (5th ed. 2015) (emphasizing the importance of “maintain[ing] the integrity of digital evidence in the lab” by creating a read-only copy prior to analysis); Jonathan L. Moore, *Time for an Upgrade: Amending the Federal Rules of Evidence to Address the Challenges of Electronically Stored Information in Civil Litigation*, 50 *Jurimetrics J.* 147, 153 (2010) (“[All electronically stored information is] prone to manipulation[;] . . . [such] alteration can occur intentionally or inadvertently.”); Int’l Org. for Standardization & Int’l Electrotechnical Comm’n, *Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence* 17 (2012) [hereinafter *ISO/IEC, Guidelines*] (emphasizing the importance of careful storage and transport techniques and noting that “[s]poliation can result from magnetic degradation, electrical degradation, heat, high or low humidity exposure, as well as shock and vibration”).

Goldfoot, *supra*, at 127-28.<sup>29</sup> And as a corollary to this fragmentation, the computer stores unseen information about any given “file” — not only metadata about when the file was created or who created it, *see* Michael W. Graves, *Digital Archaeology: The Art and Science of Digital Forensics* 94-95 (2014), but also prior versions or edits that may still exist “in the document or associated temporary files on [the] disk” — further interspersing the data corresponding to that “file” across the physical storage medium, Eoghan Casey, *Digital Evidence and Computer Crime* 507 (3d ed. 2011).

“Files,” in short, are not as discrete as they may appear to a user. Their interspersion throughout a digital storage medium, moreover, may affect the degree to which it is feasible, in a case involving search pursuant to a warrant, to fully extract and segregate responsive data from non-responsive data. To be clear, we do not suggest that it is impossible to do so in any particular or in every case; we emphasize only that in assessing the reasonableness, for Fourth Amendment purposes, of the search and seizure of digital evidence, we must be

---

<sup>29</sup> *See* Goldfoot, *supra* (“Storage media do not naturally divide into parts,” *id.* at 131; “it is difficult to agree . . . on where the subcontainers begin and end,” *id.* at 113.); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 557 (2005) (“[V]irtual files are not robust concepts. Files are contingent creations assembled by operating systems and software.”); *see also* Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex. Tech L. Rev. 1, 32 (2015) (“What does it mean to ‘delete’ data?”).

attuned to the technological features unique to digital media as a whole and to those relevant in a particular case — features that simply do not exist in the context of paper files.

These features include an additional complication affecting the validity of the file cabinet analogy: namely, that a good deal of the information that a forensic examiner may seek on a digital storage device (again, because it is a coherent and complex forensic object and not a file cabinet) does not even remotely fit into the typical user's conception of a "file." See Daniel B. Garrie & Francis M. Allegra, Fed. Judicial Ctr., *Understanding Software, the Internet, Mobile Computing, and the Cloud: A Guide for Judges* 39 (2015) ("Forensic software gives a forensic examiner access to electronically stored information (ESI) that is otherwise unavailable to a typical computer user."). Forensic investigators may, *inter alia*, search for and discover evidence that a file was deleted as well as evidence sufficient to reconstruct a deleted file — evidence that can exist in so-called "unallocated" space on a hard drive. See Casey, *supra*, at 496; Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 Harv. L. Rev. 531, 542, 545 (2005); Fed. Judicial Ctr., *supra*, at 40 ("A host of information can lie in the interstices between the allocated spaces."). They may seek responsive metadata about a user's

activities, or the manner in which information has been stored, to show such things as knowledge or intent, or to create timelines as to when information was created or accessed.<sup>30</sup> Forensic examiners will sometimes seek evidence on a storage medium that something *did not happen*: “If a defendant claims he is innocent because a computer virus committed the crime, the absence of a virus on his hard drive is ‘dog that did not bark’ negative evidence that disproves his story. . . . To prove something is not on a hard drive, it is necessary to look at every place on the drive where it might be found and confirm it is not there.”<sup>31</sup> Goldfoot, *supra*, at 141; *see also United States v. O’Keefe*, 461 F.3d 1338, 1341 (11th Cir. 2006) (“[The government’s expert] testified that the two viruses he found on [the defendant’s] computer were not capable of ‘downloading and uploading child pornography and sending out advertisements.’”).<sup>32</sup>

---

<sup>30</sup> *See Pharmacy Records v. Nassar*, 379 F. App’x 522, 525 (6th Cir. 2010) (describing testimony of a digital forensics expert in a copyright case that the number and physical location of a file on an Apple Macintosh — which saves files sequentially on its storage medium — demonstrated that the file had been back-dated).

<sup>31</sup> Indeed, in this very case, as already noted, *see supra* note 16, Ganas at one point claimed that a “software error” or “computer flaw” prevented him from recording certain income in his QuickBooks files. J.A. 467, ¶ 28. Data confirming the existence, or non-existence, of an error affecting the particular installation of a program on a given digital storage device could be, in a hypothetical case, relevant to the probity of information otherwise located thereupon.

<sup>32</sup> We note that some of these inferences may be limited to — or at least of more relevance to — traditional magnetic disk drives, which have long been the primary

Finally, because of the complexity of the data thereon and the manner in which it is stored, the nature of digital storage presents potential challenges to parties seeking to preserve digital evidence, authenticate it at trial, and establish its integrity for a fact-finder — challenges that materially differ from those in the paper file context. First, the extraction of specific data files to some other

---

digital storage technology. “Generally when data is deleted from a [traditional hard disk drive], the data is retained until new data is written onto the same location. If no new data is written over the deleted data, then the forensic investigator can recover the deleted data, albeit in fragments.” Alastair Nisbet et al., *A Forensic Analysis and Comparison of Solid State Drive Data Retention with TRIM Enabled File Systems*, Proceedings of the 11th Australian Digital Forensics Conference 103 (2013). In contrast, the technology used in solid state drives “requires a cell to be completely erased or zeroed-out before a further write can be committed,” *id.* at 104, and in part because such erasure can be time consuming, solid state drives incorporate protocols which “zero-delete data locations . . . as a matter of course,” thereby “reduc[ing] the data that can be retrieved from the drive by [a] forensic investigator,” *id.* at 103. *See also* Graeme B. Bell & Richard Boddington, *Solid State Drives: The Beginning of the End for Current Practice in Digital Forensic Recovery?*, 5 J. Digital Forensics, Sec. & L., no. 3, 2010, at 1, 12 (stating that, in connection with such storage devices, “evidence indicating ‘no data’ does not authoritatively prove that data did not exist at the time of capture”). That is not to say that studies indicate that deleted information is *never* recoverable from any model of solid state drive. *See, e.g.*, Christopher King & Timothy Vidas, *Empirical Analysis of Solid State Disk Data Retention When Used with Contemporary Operating Systems*, 8 Digital Investigation 111, 113 (2011) (citing a study suggesting that data deleted from a particular solid state drive was recoverable in certain contexts); Gabriele Bonetti et al., *A Comprehensive Black-Box Methodology for Testing the Forensic Characteristics of Solid-State Drives*, Proceedings of the 29th Annual Computer Security Applications Conference 277 (2013) (observing that, though several tested solid state drives contained no recoverable deleted data, one model contained “high[ly] recoverab[le]” quantities of such data). The point is simply that there may be material differences among different varieties of storage media that, in turn, make certain factors cited herein more or less relevant to a given inquiry.

medium can alter, omit, or even destroy portions of the information contained in the original storage medium. Preservation of the original medium or a complete mirror may therefore be necessary in order to safeguard the integrity of evidence that has been lawfully obtained or to authenticate it at trial. *Graves, supra*, at 95-96 (“[The investigator] must be able to prove that the information presented came from where he or she claims and was not altered in any way during examination, and that there was no opportunity for it to have been replaced or altered in the interim.”); *see also* *Casey, supra*, at 480 (“Even after copying data from a computer or piece of storage media, digital investigators generally retain the original evidential item in a secure location for future reference.”).<sup>33</sup> The preservation of data, moreover, is not simply a concern for law enforcement.

---

<sup>33</sup> We do not suggest that authentication of evidence from computerized records is impossible absent retention of an entire hard drive or mirror. Authentication is governed by Federal Rule of Evidence 901, which requires only that “the proponent must produce evidence sufficient to support a finding that the item is what the proponent claims it is.” Fed. R. Evid. 901(a). As we have stated, “[t]his requirement is satisfied ‘if sufficient proof has been introduced so that a reasonable juror could find in favor of authenticity or identification.’” *United States v. Pluta*, 176 F.3d 43, 49 (2d Cir. 1999) (citation omitted) (quoting *United States v. Ruggiero*, 928 F.2d 1289, 1303 (2d Cir. 1991)). “[T]he burden of authentication does not require the proponent of the evidence to rule out all possibilities inconsistent with authenticity, or to prove beyond any doubt that the evidence is what it purports to be. Rather, the standard for authentication, and hence for admissibility, is one of reasonable likelihood.” *Id.* (alteration omitted) (quoting *United States v. Holmquist*, 36 F.3d 154, 168 (1st Cir. 1994)). The weight of digital evidence admitted at trial, however, may be undermined by challenges to its integrity — challenges which proper preservation might have otherwise avoided.

Retention of the original storage medium or its mirror may also be necessary to afford criminal defendants access to that medium or its forensic copy so that, relying on forensic experts of their own, they may challenge the authenticity or reliability of evidence allegedly retrieved. *See, e.g., United States v. Kimoto*, 588 F.3d 464, 480 (7th Cir. 2009) (quoting the defendant's motion as stating: "Upon beginning their work, [digital analysis experts] advised [the defendant's] Counsel that the discovery provided to the defense did not appear to be a complete forensic copy, and that such was necessary to verify the data as accurate and unaltered.").<sup>34</sup> Defendants may also require access to a forensic copy to conduct an independent analysis of precisely what the government's forensic expert did — potentially altering evidence in a manner material to the case — or to locate exculpatory evidence that the government missed.<sup>35</sup>

---

<sup>34</sup> Where, as in this case, a mirror containing responsive data has been lawfully seized from a third-party custodian, this concern cannot be avoided simply by returning the original medium to the party from whom it was seized. A third-party custodian may need to utilize a hard drive in ways that will alter the data, and will likely have no incentive to retain a mirrored copy of drives as they once existed but that are of no further use to the custodian.

<sup>35</sup> *See Kimoto*, 588 F.3d at 480-81 ("[The defendant] argued that the failure to provide him with a complete forensic copy of all digital files impaired his ability to prepare a defense. . . . [The defendant] submitted that he should not be punished 'because the Government failed to properly preserve or maintain a digital forensic copy of the data.'"); *Casey, supra*, at 510-11 (discussing a case study in which, due to forensic investigators' own mistakes, discovery of digital evidence confirming a murder

Notwithstanding any other distinctions between this case and *Tamura*, then, the Government plausibly argues that, because digital storage media constitute coherent forensic objects with contours more complex than — and materially distinct from — file cabinets containing interspersed paper documents, a digital storage medium or its forensic copy may need to be retained, during the course of an investigation and prosecution, to permit the accurate extraction of the primary evidentiary material sought pursuant to the warrant; to secure metadata and other probative evidence stored in the interstices of the storage medium; and to preserve, authenticate, and effectively present at trial the evidence thus lawfully obtained. To be clear, we do not decide the ultimate merit of this argument as applied to the circumstances of this case.<sup>36</sup> Nor do we gainsay the privacy concerns implicated when the

---

suspect's alibi was greatly delayed); *see also id.* at 508-510 (detailing the importance of experts reporting their processes); Fed. Judicial Ctr., *supra*, at 41 (“The forensic examiner . . . generate[s] reports, detailing the protocols and processes that he or she followed . . . . The forensic reports must provide enough data to allow an independent third-party examiner to recreate the exact environment that yielded the report's findings and observations.”); Darren R. Hayes, *A Practical Guide to Computer Forensics Investigations* 116 (2015) (“[B]ecause forensics is a science, the process by which the evidence was acquired must be repeatable, with the same results.”); ISO/IEC, *Guidelines*, *supra*, at 7 (emphasizing the importance of repeatability and reproducibility).

<sup>36</sup> That said, it is important to correct a misunderstanding in the dissent's analysis, as it pertains to these factors and their application here. The dissent suggests that the Government can have had no interest in retention, as “[t]he agents could not

government retains a hard drive or forensic mirror containing personal information irrelevant to the ongoing investigation, even if such information is never viewed. We discuss the aptness and limitations of Ganias's analogy and

---

have been keeping non-responsive files [in order to authenticate and defend the probity of responsive files] for the purpose of proceeding against Ganias, as [in December 2004] they did not yet suspect [him] of criminal wrongdoing." Dissent at 22. This argument misunderstands the Government's position: the Government was not retaining the mirrors in late 2004 and 2005 in the hopes of proceeding against Ganias; it was retaining the mirrors as part of its ongoing investigation of James McCarthy and his two companies, AB and IPM — an investigation that would culminate in an indictment of McCarthy in 2008 secured through extensive reliance on responsive data recovered from the mirrored copies of Ganias's hard drives. The dissent's focus on Ganias, the owner of the hard drives the Government mirrored, and not McCarthy, a third-party defendant, thus permits the dissent to dismiss out-of-hand Government interests that, properly viewed, are significant — whether or not ultimately dispositive. *See* Dissent at 24 ("As a practical matter, a claim of data tampering would easily fall flat where, as here, the owner kept his original computer and the Government gave him a copy of the mirror image."); *id.* at 25-26 (dismissing the Government's *Brady* concern by noting that "[t]he Government is essentially arguing that it must hold on to the materials so that it can give them back to the defendant," a concern that the dissent argues "can be obviated simply by returning the non-responsive files to the defendant in the first place"). Perhaps in some situations, in which the owner of computerized data seized pursuant to a search warrant is the expected defendant in a criminal proceeding, problems of authentication or probity could be handled by stipulations, and *Brady* issues might be mooted by the return of the data to the defendant — though we express no view on those questions. As this case illustrates, however, when the owner of hard drives mirrored by the government is a third party who is not the expected target of the investigation, the government's interests in retention take on an additional layer of complexity. A stipulation with Ganias about the authenticity or probity of data extracted from his computers would not have affected the ability of the original targets of the investigation to raise challenges to authenticity or probity. Nor would returning the mirrors to Ganias — who at that point, absent a stipulation to the contrary, could presumably have destroyed or altered them, intentionally or accidentally — have protected the interests of those anticipated defendants in conducting their own forensic examination of the data in search of exculpatory evidence or to replicate and criticize the Government's inspection procedures.

the Government's response simply to highlight the complexity of the relevant questions for future cases and to underscore the importance, in answering such questions, of engaging with the technological specifics.<sup>37</sup>

---

<sup>37</sup> Of course, engaging with the specifics requires acknowledging and emphasizing that technologies rapidly evolve, and that the specifics change. See John Sammons, *The Basics of Digital Forensics* 170 (2012) (commenting that digital forensics faces the "blinding speed of technology [and] new game-changing technologies such as cloud computing and solid state hard drives . . . just to name a few"). In discussing the technological specifics of computer hard drives, we have primarily addressed a particular form of electronic storage that has become conventional. See *supra* note 32. Newer forms of emerging storage technology, or future developments, may work differently and thus present different challenges. See, e.g., Bell & Boddington, *supra*, at 3, 6, 14 (observing that "the peculiarity of 'deleted, but not forgotten' data which so often comes back to haunt defendants in court is in many ways a bizarre artefact of hard drive technology" and that increasingly popular solid state drives can "modify themselves very substantially without receiving instructions to do so from a computer," and thus predicting that "recovery of deleted files and old metadata will become extremely difficult, if not impossible" as solid state storage devices utilizing a particular deletion protocol called "TRIM" become more prevalent); King & Vidas, *supra*, at 111 ("We show that on a TRIM-enabled [solid state drive], using an Operating System (OS) that supports TRIM, . . . in most cases no data can be recovered."); *id.* at 113 ("[M]ost [solid state drive] manufacturers have a TRIM-enabled drive model currently on the market."). But see Bonetti et al., *supra*, at 270-71, 278 (making clear that solid state drives, which differ considerably among models and vendors, may yield differing levels of deleted-file recoverability, depending upon their utilization of TRIM and other deletion protocols, erasing patterns, compression, and wear leveling protocols). Solid state drives, of course, are just one example. Cf. Bell & Boddington, *supra*, at 3 ("It is . . . in the nature of computing that we perceive regular paradigm shifts in the ways that we store and process information."). The important point is that considerations discussed in this opinion may well become obsolete at some future point, the challenges facing forensic examiners and affected parties may change, and courts dealing with these problems will need to become conversant with the particular forms of technology involved in a given case and the evidentiary challenges presented by those forms.

In emphasizing such specifics, we reiterate that we do not mean to thereby minimize or ignore the privacy concerns implicated when a hard drive or forensic mirror is retained, even pursuant to a warrant. The seizure of a computer hard drive, and its subsequent retention by the government, can give the government possession of a vast trove of personal information about the person to whom the drive belongs, much of which may be entirely irrelevant to the criminal investigation that led to the seizure. Indeed, another weakness of the file cabinet analogy is that no file cabinet has the capacity to contain as much information as the typical computer hard drive. In 2005, Professor Orin Kerr noted that the typical personal computer hard drive had a storage capacity of about eighty gigabytes, which he estimated could hold text files equivalent to the “information contained in the books on one floor of a typical academic library.” Kerr, *Searches and Seizures in a Digital World*, *supra*, at 542. By 2011, computers were being sold with one terabyte of capacity — about twelve times the size of Professor Kerr’s library floor. Paul Ohm, *Response, Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 Va. L. Rev. In Brief 1, 6 (2011). The *New York Times* recently reported that commercially available storage devices can hold “16 petabytes of data, roughly equal to 16 billion thick books.” Quentin

Hardy, *As a Data Deluge Grows, Companies Rethink Storage*, N.Y. Times, Mar. 15, 2016, at B3.

Moreover, quantitative measures fail to capture the significance of the data kept by many individuals on their computers. Tax records, diaries, personal photographs, electronic books, electronic media, medical data, records of internet searches, banking and shopping information — all may be kept in the same device, interspersed among the evidentiary material that justifies the seizure or search. *Cf. Riley v. California*, 134 S. Ct. 2473, 2489-90 (2014) (explaining that even microcomputers, such as cellphones, have “immense storage capacity” that may contain “every piece of mail [people] have received for the past several months, every picture they have taken, or every book or article they have read,” which can allow the “sum of an individual’s private life [to] be reconstructed”); *United States v. Galpin*, 720 F.3d 436, 446 (2d Cir. 2013) (“[A]dvances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain.”). While physical searches for paper records or other evidence may require agents to rummage at least cursorily through much private material, the reasonableness of seizure and subsequent retention

by the government of such vast quantities of irrelevant private material was rarely if ever presented in cases prior to the age of digital storage, and has never before been considered justified, or even practicable, in such cases. Even as we recognize that search and seizure of digital media is, in some ways, distinct from what has come before, we must remain mindful of the privacy interests that necessarily inform our analysis.<sup>38</sup>

We note, however, that parties with an interest in retained storage media are not without recourse. As noted above, Ganas never sought the return of any seized material, either by negotiating with the Government or by motion to the court. Though negotiated stipulations regarding the admissibility or integrity of evidence may not always suffice to satisfy reasonable interests of the government

---

<sup>38</sup> The dissent extensively addresses these privacy interests. As this opinion makes clear, we do not disagree with the proposition that the seizure and retention of computer hard drives or mirrored copies of those drives implicate such concerns and raise significant Fourth Amendment questions. We do not agree, however, for reasons we have also discussed at length, with the dissent's dismissal of the countervailing government concerns. However these issues are ultimately resolved, we believe that the Government's arguments are, at a minimum, sufficiently forceful that it is unwise to try to reach definitive conclusions about the constitutional issues in a case that can be decided on other grounds.

in retention during the pendency of an investigation,<sup>39</sup> such stipulations may make return feasible in a proper case, and can be explored.

A person from whom property is seized by law enforcement may move for its return under Federal Rule of Criminal Procedure 41(g).<sup>40</sup> Rule 41(g) permits a defendant or any “person aggrieved” by either an unlawful or *lawful* deprivation of property, *see United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1173 (9th Cir. 2010) (en banc) (per curiam), to move for its return, Fed. R. Crim. P. 41(g). Evaluating such a motion, a district court “must receive evidence on any factual issue necessary to decide the motion,” and, in the event that the motion is granted, may “impose reasonable conditions to protect access to the property and its use in later proceedings.” *Id.* Since we resolve this case on other

---

<sup>39</sup> For instance, as we have previously noted, where, as here, the owner of the records is not (at least at the time of the seizure) the target of the investigation, a stipulation from that party may not serve the government’s need to establish the authenticity or integrity of evidence it may seek to use, and access to the records by that party will not necessarily satisfy the need of potential future defendants to test the processes used by the government to extract or accurately characterize data culled from a hard drive. In some cases, however, negotiated solutions may be practicable.

<sup>40</sup> Rule 41(g) provides as follows:

**Motion to Return Property.** A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property’s return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.

grounds, we need not address whether Ganias's failure to make such a motion forfeited any Fourth Amendment objection he might otherwise have had to the Government's retention of the mirrors. But we agree with the district court that, as a pragmatic matter, such a motion "would have given a court the opportunity to consider 'whether the government's interest could be served by an alternative to retaining the property,' and perhaps to order the [mirrors] returned to Ganias, all while enabling the court to 'impose reasonable conditions to protect access to the property and its use in later proceedings.'" *Ganias*, 2011 WL 2532396, at \*8 (citation omitted) (first quoting *In re Smith*, 888 F.2d 167, 168 (D.C. Cir. 1989) (per curiam); then quoting Fed. R. Crim. P. 41(g)).

Rule 41(g) thus provides a potential mechanism, in at least some contexts, for dealing with the question of retention at a time when the government may be expected to have greater information about the data it seeks and the best process through which to search and present that data in court. It is worth observing, then, that Rule 41(g) constitutes a statutory solution (as opposed to a purely judicially constructed one) to at least one facet of the retention problem.<sup>41</sup>

---

<sup>41</sup> The advisory committee notes to the 2009 amendments to Federal Rule of Criminal Procedure 41(e)(2)(B) contemplate that Rule 41(g) may indeed constitute such a solution. Regarding specifically the seizure of electronic storage media or the search

Statutory approaches, of course, do not relieve courts from their obligation to interpret the Constitution; nevertheless, such approaches have, historically, provided one mechanism for safeguarding privacy interests while, at the same time, addressing the needs of law enforcement in the face of technological change. Indeed, when Congress addressed wiretapping in the Omnibus Crime Control and Safe Streets Act of 1968, the Senate Judiciary Committee issued a report reflecting precisely this ambition — to provide a framework through which law enforcement might comport with the demands of the Constitution and meet important law enforcement interests. *See* S. Rep. No. 90-1097, at 66-76 (1968) (describing the construction of the then-Omnibus Crime Control and Safe Streets of Act of 1967, which laid out comprehensive rules for when and how law enforcement could intercept wire and oral communications through electronic surveillance, as a Congressional attempt to respond to and synthesize, first, technological change, *id.* at 67, second, ineffective or unclear state statutory

---

of electronically stored information, the advisory committee notes observe that though the rule does not create

a presumptive national or uniform time period within which . . . off-site copying or review of . . . electronically stored information would take place, . . . [i]t was not the intent of the amendment to leave the property owner without . . . a remedy[:]. . . Rule 41(g) . . . provides a process for the “person aggrieved” to seek an order from the court for a return of the property, including storage media or electronically stored information, under reasonable circumstances.

regimes, *id.* at 69, third, evolving Supreme Court precedent, *id.* at 74-75, and fourth, law enforcement concerns, *id.* at 70); *see also id.* at 66 (“Title III has as its dual purpose (1) protecting the privacy of wire and oral communications, and (2) delineating on a uniform basis the circumstances and conditions under which the interception of wire and oral communications may be authorized.”). The Act did not seek to supplant the role of the courts, nor could it have done so, but it did demonstrate the intuitive proposition that Congress can and should be a partner in the process of fleshing out the contours of law-enforcement policy in a shifting technological landscape. In acknowledging the role of Rule 41(g), then, we seek also to suggest that search and seizure of electronic media may, no less than wiretapping, merit not only judicial review but also legislative analysis; courts need not act alone.

As we have said, we need not resolve the ultimate question whether the Government’s retention of forensic copies of Ganias’s hard drives during the pendency of its investigation violated the Fourth Amendment. We conclude, moreover, that we should not decide this question on the present record, which does not permit a full assessment of the complex and rapidly evolving technological issues, and the significant privacy concerns, relevant to its

consideration.<sup>42</sup> Having noted Ganias's argument, we do not decide its merits.

We instead turn to the question of good faith.

---

<sup>42</sup> The dissent faults us for our caution in this regard, suggesting that "the prevailing scholarly consensus has been that the [original *Ganias*] panel largely got it right." Dissent at 5 n.5. With respect, the dissent mischaracterizes the scholarly response. As an initial matter, the dissent cites Professor Kerr as having concluded that the panel "largely got it right." *Id.* In fact, Kerr's analysis of the original panel opinion is generally critical, not complimentary. See Kerr, *Executing Warrants for Digital Evidence, supra*, at 32 (critiquing the panel for going too far and thus offering a "particularly strong version" of Kerr's approach). Assessing the original panel's analysis, Kerr first concludes that, given the technological contours of electronic media, an affirmative obligation to delete could be "difficult to implement," just as it could be difficult to ascertain at what point in the process such a "duty [would be] triggered." *Id.* Second, Kerr concludes that — to the degree that restrictions should be placed upon what the government may do with non-responsive data that must, for pragmatic reasons, be retained — a restriction preventing the government from viewing data pursuant to a search warrant acquired with independent probable cause is unnecessary "to restore the basic limits of search warrants in a world of digital evidence." *Id.* at 33.

Apart from this citation to Kerr and to two student notes (which reach differing conclusions about the merits of the panel opinion), the articles the dissent cites (as is evident from the carefully worded parentheticals the dissent itself provides) are not evaluations of the original panel opinion, but instead provide largely descriptive accounts of the opinion and its relation to other case law in the context of making other points. The signed article that comes the closest to providing a normative critique of the panel's opinion concludes that "*perhaps* the panel's answer is broadly the right answer," but rejects the panel's — and the dissent's — reasoning. Stephen E. Henderson, *Fourth Amendment Time Machines (and What They Might Say About Police Body Cameras)*, 18 U. Pa. J. Const. L. 933, 948 (2016) (emphasis added); see *id.* at 947 (concluding that, because "in 2003 and in 2006 the government obtained a warrant demonstrating particularized suspicion towards Ganias's data, and in each instance agents thereafter only looked for the responsive data," it was inapt for the original panel to conclude that the Government's position would transform a warrant for electronic data into a "general warrant"). We do not opine on these issues here, but we see no scholarly consensus on the complicated questions implicated in this case that would suggest caution is ill-advised in a matter where these questions need not be answered to reach a resolution. Caution, although not always satisfying, is sometimes the most appropriate approach.

### III

The Government argues that, because it acted in good faith throughout the pendency of this case, any potential violation of the Fourth Amendment does not justify the extraordinary remedy of suppression. *See Davis v. United States*, 564 U.S. 229, 237 (2011) (noting the “heavy toll” exacted by suppression, which “requires courts to ignore reliable, trustworthy evidence,” and characterizing suppression as a “bitter pill,” to be taken “only as a ‘last resort’” (quoting *Hudson v. Michigan*, 547 U.S. 586, 591 (2006))); accord *United States v. Clark*, 638 F.3d 89, 99 (2d Cir. 2011). In particular, the Government urges that its “reliance on the 2006 warrant,” which it obtained after disclosing to the magistrate judge all relevant facts regarding its retention of the mirrored files, “fits squarely within the traditional *Leon* exception for conduct taken in reliance on a search warrant issued by a neutral and detached magistrate judge.”<sup>43</sup> Government Br. at 59; *see Leon*, 468 U.S. at 922. For the following reasons, we agree.

---

<sup>43</sup> The Government also contends: (1) that it relied in good faith on the 2003 warrant in retaining the mirrors; and (2) that its behavior was in no way culpable, rendering exclusion inappropriate, *see* Government Br. at 51; *see also Herring v. United States*, 555 U.S. 135, 144 (2009) (“[T]he exclusionary rule serves to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence.”); accord *Davis*, 546 U.S. at 237. Given our conclusion that the Government relied in good faith on the 2006 warrant, we need not address these additional arguments.

In *Leon*, the Supreme Court determined that the exclusion of evidence is inappropriate when the government acts “in objectively reasonable reliance” on a search warrant, even when the warrant is subsequently invalidated. 468 U.S. at 922; *see also Clark*, 638 F.3d at 100 (“[I]n *Leon*, the Supreme Court strongly signaled that most searches conducted pursuant to a warrant would likely fall within its protection.”). Such reliance, however, must be *objectively reasonable*. *See Leon*, 468 U.S. at 922-23 (“[I]t is clear that in some circumstances the officer will have no reasonable grounds for believing that the warrant was properly issued.” (footnote omitted)). Thus, to assert good faith reliance successfully, officers must, *inter alia*, disclose all potentially adverse information to the issuing judge. *See United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir.) (“The good faith exception to the exclusionary rule does not protect searches by officers who fail to provide all potentially adverse information to the issuing judge . . .”), *aff’d and amended*, 91 F.3d 331 (2d Cir. 1996) (per curiam); *see also United States v. Thomas*, 757 F.2d 1359, 1368 (2d Cir. 1985) (finding good faith reliance on a warrant, under *Leon*, where officers, first, committed a constitutional violation they did not reasonably know, at the time, was unconstitutional — a warrantless canine sniff — and second, in relying on evidence from this sniff in a warrant application,

fully revealed the fact of the canine sniff to a magistrate judge), *cert. denied by Fisher v. United States*, 474 U.S. 819 (1985) and *Rice v. United States*, 479 U.S. 818 (1986).

Ganias argues that reliance on the 2006 warrant is misplaced for two reasons. First, he urges that the alleged constitutional violation here (unlawful retention of the mirrored drives) had “long since” ripened into a violation by April 2006, when the second warrant was obtained, Appellant Br. at 55-56, and attests that “[n]othing [in *Leon*] suggests that the police, *after* they engage in misconduct, can then ‘launder their prior unconstitutional behavior by presenting the fruits of it to a magistrate,’” *id.* at 56 (quoting *State v. Hicks*, 707 P.2d 331, 333 (Ariz. Ct. App. 1985)). Second, Ganias argues that, even if “a subsequent warrant can ever appropriately purge the taint of an earlier violation, the agent must, at the very least, ‘provide all potentially adverse information’ regarding the earlier illegality ‘to the issuing [magistrate] judge,’” a requirement that he argues was not satisfied here. *Id.* at 58 (quoting *Reilly*, 76 F.3d at 1280). Ganias’s arguments are unavailing.

First, Ganias relies on this Court’s decision in *Reilly* to argue categorically that agents who have engaged in a predicate Fourth Amendment violation may

not rely on a subsequently issued warrant to establish good faith. *Reilly*, however, stands for no such thing. In *Reilly*, officers unlawfully intruded on the defendant's curtilage, discovering about twenty marijuana plants, before they departed and obtained a search warrant based on a "bare-bones" description of their intrusion and resulting observations which this Court found "almost calculated to mislead." *Reilly*, 76 F.3d at 1280; *see also id.* ("[The affidavit] simply . . . stated that [the officers] walked along Reilly's property until they found an area where marijuana plants were grown. It did not describe this area to the Judge[,] . . . [and it] gave no description of the cottage, pond, gazebo, or other characteristics of the area. . . . [The omitted information] was crucial. Without it, the issuing judge could not possibly make a valid assessment of the legality of the warrant that he was asked to issue."). We rejected the government's argument that the officers were entitled to rely on the warrant, noting that the officers had "undert[aken] a search that caused them to invade what they could not fail to have known was potentially . . . curtilage," and that they thereafter "failed to provide [the magistrate issuing the warrant] with an account of what they did," so that the magistrate was unable to ascertain whether the evidence on which the officers relied in seeking the warrant was

“itself obtained illegally and in bad faith.” *Id.* at 1281. In such circumstances, *Leon* did not — and does not — permit good faith reliance on a warrant. *See Leon*, 468 U.S. at 923 (observing that an officer’s reliance on a warrant is not *objectively reasonable* if he “misled [the magistrate with] information in an affidavit that [he] knew was false or would have known was false except for his reckless disregard of the truth”).

The present case, however, is akin not to *Reilly*, but to this Court’s decision in *Thomas*, which the *Reilly* panel carefully distinguished, while reaffirming. *See Reilly*, 76 F.3d at 1281-82. In *Thomas*, an agent, acting without a warrant, used a dog trained to detect narcotics to conduct a “canine sniff” at a dwelling. 757 F.2d at 1367. The agent presented evidence acquired as a result of the sniff to a “neutral and detached magistrate” who, on the basis of this and other evidence, determined that the officer had probable cause to conduct a subsequent search of the dwelling in question. *Id.* at 1368. The defendant moved to suppress the evidence found in executing the search warrant, arguing that the antecedent canine sniff constituted a warrantless, unconstitutional search and that the evidence acquired from that sniff was dispositive to the magistrate judge’s finding of probable cause. *See id.* at 1366. This Court agreed on both counts: first

deciding, as a matter of first impression in our Circuit, that the canine sniff at issue constituted a search, *id.* at 1367, and second determining that, absent the evidence acquired from this search, the warrant was not supported by probable cause, *id.* at 1368. The *Thomas* panel nevertheless concluded that suppression was inappropriate because the agent's reliance on the warrant was objectively reasonable: "The . . . agent brought his evidence, including [a factual description of the canine sniff], to a neutral and detached magistrate. That magistrate determined that probable cause to search existed, and issued a search warrant. There is nothing more the officer could have or should have done under these circumstances to be sure his search would be legal." *Id.*

*Reilly* carefully distinguished *Thomas*, and in a manner that makes apparent that it is *Thomas* that is dispositive here. First, the *Reilly* panel noted that *Thomas* was unlike *Reilly*, in that the agent in *Thomas* disclosed all crucial facts for the legal determination in question to the magistrate judge. *Reilly*, 76 F.3d at 1281. Then, the *Reilly* panel articulated another difference: while in *Reilly*, "the officers undertook a search that caused them to invade what they could not fail to have known was potentially *Reilly's* curtilage," in *Thomas*, the agent "did not have any significant reason to believe that what he had done [conducting the

canine sniff] was unconstitutional.” *Id.*; see also *id.* (“[U]ntil *Thomas* was decided, no court in this Circuit had held that canine sniffs violated the Fourth Amendment.”). Thus, the predicate act in *Reilly* tainted the subsequent search warrant, whereas the predicate act in *Thomas* did not. The distinction did not turn on whether the violation found was *predicate*, or prior to, the subsequent search warrant on which the officers eventually relied, but on whether the officers’ reliance on the warrant was reasonable.

Contrary to Ganas’s argument, then, it is not the case that good faith reliance on a warrant is never possible in circumstances in which a predicate constitutional violation has occurred. The agents in *Thomas* committed such a violation, but they had no “significant reason to believe” that their predicate act was indeed unconstitutional, *Reilly*, 76 F.3d at 1281, and the issuing magistrate was apprised of the relevant conduct, so that the magistrate was able to determine whether any predicate illegality precluded issuance of the warrant. In such circumstances, invoking the good faith doctrine does not “launder [the agents’] prior unconstitutional behavior by presenting the fruits of it to a magistrate,” as Ganas suggests. Appellant Br. at 56 (quoting *Hicks*, 707 P.2d at 333). In such cases, the good faith doctrine simply reaffirms *Leon*’s basic lesson:

that suppression is inappropriate where reliance on a warrant was “objectively reasonable.” *Leon*, 468 U.S. at 922.<sup>44</sup>

Such is the case here. First, Agent Hosney provided sufficient information in her affidavit to apprise the magistrate judge of the pertinent facts regarding the retention of the mirrored copies of Ganias’s hard drives — the alleged constitutional violation on which he relies. Agent Hosney explained that the mirror images in question had been “seized on November 19, 2003 from the offices of Taxes International,” J.A. 461, ¶ 7; that information material to the initial investigation of a third party had been located on the mirrors and “analyzed in detail,” J.A. 464, ¶ 15; that Ganias was not, at the time of the original seizure, under investigation, J.A. 461, ¶ 3; that, “[p]ursuant to [that initial warrant],” Agent Hosney could not search Ganias’s personal or business files as

---

<sup>44</sup> Insofar as Ganias argues that *Thomas’s* and *Reilly’s* holdings are limited to when the alleged predicate violation is a *search* that taints the warrant, but do not extend to circumstances in which the alleged predicate violation is a seizure or unlawful retention, we discern no justification for this distinction. But for the canine search in *Thomas* — the predicate violation — there would have been no subsequent warrant pursuant to which the government searched the dwelling and on whose legality it relied in conducting that search. But for the retention in this case — the alleged predicate violation — there could have been no subsequent search warrant pursuant to which the Government searched the relevant evidence and on whose legality the Government relied in conducting that search. To credit Ganias’s distinction would be to replace the underlying directive that reliance on a warrant be “objectively reasonable,” *Leon*, 468 U.S. at 922, with an arbitrary formalism.

the warrant authorized search only of “files for [AB] and IPM,” J.A. 464, ¶ 14; and that Ganias’s personal data — which Agent Hosney was not authorized to search — was *on those mirrored drives*, J.A. 467, ¶ 27, and thus, *a fortiori*, had been there for the past two and a half years. The magistrate judge was thus informed of the fact that mirrors containing data non-responsive to the 2003 warrant had been retained for several years past the initial execution of that warrant and, to the degree it was necessary, that data responsive to the 2003 warrant had been analyzed in detail. The magistrate therefore had sufficient information on which to determine whether such retention precluded issuance of the 2006 warrant. *Cf. Thomas*, 757 F.2d at 1368 (“The magistrate, whose duty it is to interpret the law, determined that the canine sniff could form the basis for probable cause . . .”).

Ganias disagrees, arguing, in particular, that, though Agent Hosney alerted the magistrate that the mirrors had been retained for several years; that data responsive to the original warrant had been both located and extensively analyzed; and that those of Ganias’s QuickBooks files that Agent Hosney wanted to search were non-responsive to the original warrant, the Hosney affidavit did not go far enough in that it failed to disclose that the agents “had been retaining the non-responsive records for a full 16 months *after* the files within the

November 2003 warrant's scope had been identified." Appellant Br. at 60. As an initial matter, the Government *did* alert the magistrate that it had located responsive data on the mirrors *and* conducted extensive analysis of that responsive material, and it is not clear what else the Government should have said: the district court did not determine — nor does the record show — that by January 2005, as Ganas contends, the Government had determined, as a forward-looking matter, that it had performed all forensic searches of data responsive to the 2003 warrant that might prove necessary over the course of its investigation. *Compare* J.A. 322 (Q: "So it's fair to say that as of mid-December [2004], your forensic analysis was completed at that time?" Agent Chowaniec: "That's correct, of the computers."), *with* J.A. 324 (Q: "Did you know you wouldn't require further analysis by Greg Norman or any other examiner at the Army lab in Georgia after December of 2004?" Agent Chowaniec: "No."); *see supra* note 12. Nor would it be reasonable to expect additional detail in the affidavit on this point, even assuming Ganas's contention to be correct that the Government had both finished its segregation *and* provided insufficient facts to alert the magistrate judge to that reality, given the dearth of precedent suggesting its relevance. *Cf. Clark*, 638 F.3d at 105 ("[W]here the need for

specificity in a warrant or warrant affidavit on a particular point was not yet settled or was otherwise ambiguous, we have declined to find that a well-trained officer could not reasonably rely on a warrant issued in the absence of such specificity.”); *cf. Reilly*, 76 F.3d at 1280 (noting that the affidavit in that case, in clear contrast to the affidavit in this one, was “almost calculated to mislead”).

Second, here, as in *Thomas*, it is also clear that the agents, as the panel put it in *Reilly*, “did not have any significant reason to believe that what [they] had done was unconstitutional,” *Reilly*, 76 F.3d at 1281 — that their retention of the mirrored hard drives, while the investigation was ongoing, was anything but routine. At the time of the retention, no court in this Circuit had held that retention of a mirrored hard drive during the pendency of an investigation could violate the Fourth Amendment, much less that such retention would do so in the circumstances presented here. *See id.* (noting that suppression was inappropriate in *Thomas* in part because no relevant precedent established that canine sniffs of a dwelling “violated the Fourth Amendment”).<sup>45</sup> Moreover, as noted above, the

---

<sup>45</sup> The closest decision Ganas can locate is *United States v. Tamura*, 694 F.2d at 594-95, an out-of-circuit case that concerned intermingled paper files, the removal of which was unauthorized and the return of which had been vigorously sought by the affected parties. Whatever relevance that case may have by analogy, it is not sufficient to alert a reasonable agent to the existence of a serious Fourth Amendment problem: for to suggest that a holding applicable to retaining *intermingled paper files* specifically

2003 warrant authorized the lawful seizure not merely of particular records or data, but of the hard drives themselves, or in the alternative the creation of mirror images of the drives to be removed from the premises for later forensic evaluation, and set no greater limit on the Government's retention of those materials than on any other evidence whose seizure it authorized.

Finally, the record here is clear that the agents acted reasonably throughout the investigation. They sought authorization in 2003 to seize the hard drives and search them off-site; they minimized the disruption to Ganas's business by taking full forensic mirrors; they searched the mirrors only to the extent authorized by, first, the 2003 warrant, and then the warrant issued in 2006; they were never alerted that Ganas sought the return of the mirrors; and they alerted the magistrate judge to these pertinent facts in applying for the second warrant. In short, the agents acted reasonably in relying on the 2006 warrant to search for evidence of Ganas's tax evasion. This case fits squarely within *Leon* so that, assuming, *arguendo*, that a Fourth Amendment violation occurred, suppression was not warranted.

---

demanded to be returned clearly resolves a question about retention of a *physical digital storage medium* (the return of which had been neither suggested nor requested) would be "like saying a ride on horseback is materially indistinguishable from a flight to the moon." *Riley*, 134 S. Ct. at 2488.

\* \* \*

We conclude that the Government relied in good faith on the 2006 search warrant and thus AFFIRM the judgment of the district court. Given this determination, we do not reach the specific Fourth Amendment question posed to us today.

COMMONWEALTH OF MASSACHUSETTS

# Supreme Judicial Court

No. SJC-12938

---

Commonwealth of Massachusetts

*Appellant*

v.

Dondre Snow,

*Defendant-Appellee.*

---

ON APPEAL FROM A JUDGMENT OF  
THE SUFFOLK SUPERIOR COURT

---

**BRIEF AMICI CURIAE OF THE AMERICAN CIVIL LIBERTIES  
UNION OF MASSACHUSETTS, INC. AND THE ELECTRONIC  
FRONTIER FOUNDATION IN SUPPORT OF THE APPELLEE**

---

Jennifer Lynch (CA 240701)  
Andrew Crocker (CA 291596)  
Mark Rumold (CA 279060)  
Hannah Zhao (NY 5468673)  
ELECTRONIC FRONTIER FOUNDATION  
815 Eddy Street  
San Francisco, CA 94109  
(415) 436-9333  
jlynch@eff.org

Matthew R. Segal (BBO #654489)  
Jessie J. Rossman (BBO 670685)  
Jessica J. Lewis (BBO #704229)  
AMERICAN CIVIL LIBERTIES UNION  
FOUNDATION OF MASSACHUSETTS, INC.  
211 Congress Street  
Boston, MA 02110  
(617) 482-3170  
jrossman@aclum.org

AUGUST 28, 2020

**TABLE OF CONTENTS**

TABLE OF AUTHORITIES..... 4

CORPORATE DISCLOSURE STATEMENTS..... 7

STATEMENT OF INTERESTS OF AMICI..... 9

INTRODUCTION..... 10

STATEMENTS OF THE FACTS AND CASE..... 12

SUMMARY OF ARGUMENT..... 16

ARGUMENT..... 17

    I.    Cell phones are ubiquitous features of everyday life, with the capacity to store vast amounts of personal data. .... 17

        A. Cell phones contain a vast amount of private data about their users..... 18

        B. Cell phones are unique tools for exercising constitutional rights and conducting private communications..... 20

    II.   This Court has determined that the vast storage and communications capacities of cell phones cannot automatically establish probable cause to search and seize a person’s cell phone. .... 23

        A. The Supreme Court has limited searches of cell phones incident to arrest because they contain vast, private, and sensitive information..... 23

        B. *White* requires probable cause to believe that particularized evidence related to the crime under investigation exists on the cell phone.. 25

    III. This Court should reaffirm *White*’s holding that police need particularized evidence connecting the cell phone to be searched with the crime under investigation. .... 27

        A. Mere presence and use of a cell phone at the scene of an arrest fails to establish probable cause to search the device..... 27

B. The Commonwealth's inability to identify a  
timeframe or location for any alleged evidence  
on the phone further underscores their lack  
of probable cause..... 32

C. The Commonwealth's approach threatens privacy. 34

CONCLUSION..... 37

CERTIFICATE OF COMPLIANCE..... 39

AFFIDAVIT OF SERVICE..... 39

TABLE OF AUTHORITIES

CASES

*Buckham v. State*,  
185 A.3d 1 (Del. 2018) ..... 28, 31

*Carpenter v. United States*,  
138 S. Ct. 2206 (2018) ..... 9

*Commonwealth v. Almonor*,  
482 Mass. 35 (2019) ..... 9

*Commonwealth v. Arthur*,  
94 Mass. App. Ct. 161 (2018) ..... 30

*Commonwealth v. Augustine*,  
472 Mass. 448 (2015) ..... 9, 24

*Commonwealth v. Broom*,  
474 Mass. 486 (2016) ..... 30

*Commonwealth v. Dorelas*,  
473 Mass. 496 (2016) ..... 17, 23

*Commonwealth v. Evelyn*,  
SJC-12808 (2020) ..... 9

*Commonwealth v. Freiberg*,  
405 Mass. 282 (1989) ..... 34

*Commonwealth v. Goncalves-Mendez*,  
484 Mass. 80 (2020) ..... 32

*Commonwealth v. Holley*,  
478 Mass. 508 (2017) ..... 29

*Commonwealth v. Jordan*,  
91 Mass. App. Ct. 743 (2017) ..... 29, 31, 32

*Commonwealth v. Morin*,  
478 Mass. 415 (2017) ..... 28, 29

*Commonwealth v. Pope*,  
354 Mass. 625 (1968) ..... 32

*Commonwealth v. Snow*,  
96 Mass. App. Ct. 672 (2019) ..... 31

*Commonwealth v. White*,  
475 Mass. 583 (2016) ..... *passim*

<i>Glik v. Cunniffe</i> , 655 F.3d 78 (1st Cir. 2011) .....	21
<i>Riley v. California</i> , 573 U.S. 373 (2014) .....	<i>passim</i>
<i>Ybarra v. Illinois</i> , 444 U.S. 851 (1979) .....	37

**STATUTES, REGULATIONS AND RULES**

18 U.S.C. 2102(b).....	36
Mass. Gen. Laws ch. 269 § 1-2.....	36

**OTHER AUTHORITIES**

A. Smith, Pew Research Center, <i>Smartphone Ownership—2013 Update</i> (June 5, 2013) .....	18
Aaron Smith, <i>Americans’ experiences with data security</i> , Pew Research Center (Jan. 26, 2017) .....	20
Andrew Perrin and Erica Turner, <i>Smartphones help blacks, Hispanics bridge some - but not all - digital gaps with whites</i> , Pew Research Center (Aug. 20, 2019) ..	22
Bill Chappell, <i>Fort Worth Police Drop Rioting Charges Against Protesters</i> , NPR (June 9, 2020) .....	36
BPD News, <i>BPD Confirms Fifty-Three Arrests Made and One Summons Issued Following Protests in Boston</i> (June 1, 2020) .....	35
Emily A. Vogels, <i>Millennials stand out for their technology use, but older generations also embrace digital life</i> , Pew Research Center (Sept. 9, 2019).	18
Monica Anderson & Emily A. Vogels, <i>Americans turn to technology during COVID-19 outbreak</i> , Pew Research Center (March 31, 2020) .....	22
Ryan Deto, <i>Pittsburgh’s first two BLM protests led to dozens of arrests; about 90% of those charges have been dropped</i> , Pittsburgh City Paper (June 19, 2020) ...	36
Samantha Fields, <i>What it can cost to get arrested at a protest</i> , Marketplace (June 10, 2020) .....	35
Sarah Perez, <i>Report: Smartphone owners are using 9 apps per day, 30 per month</i> , TechCrunch (May 4, 2017) ...	19

Sujeong Lim, *Average Storage Capacity in Smartphones to Cross 80GB by End-2019*, Counterpoint (Mar. 16, 2019) ..... 19

US Virtual Care Visits To Soar To More Than 1 Billion, Forrester (Apr. 10, 2020). .... 22

Whitney Woodworth, *Criminal charges dismissed against 14 arrested at Black Lives Matter protests*, Statesman Journal (June 29, 2020). .... 36

**CONSTITUTIONAL PROVISIONS**

Mass. Declarations of Rights, Art. 14..... *passim*

U.S. Const. amend. 4..... *passim*

## **CORPORATE DISCLOSURE STATEMENTS**

Pursuant to Supreme Judicial Court Rule 1:21, the American Civil Liberties Union of Massachusetts, Inc. (ACLUM) and the Electronic Frontier Foundation (EFF) represent that they are 501(c)(3) organizations under the laws of the Commonwealth of Massachusetts. ACLUM and EFF do not issue any stock or have any parent corporation, and no publicly held corporation owns stock in ACLUM or EFF.

**PREPARATION OF AMICI BRIEF**

Pursuant to Mass. R. App. 17(c)(5), as amended, 426 Mass. 1602 (1998), amici and their counsel declare that:

(a) no party or a party's counsel authored this brief in whole or in part;

(b) no party or a party's counsel contributed money to fund preparing or submitting the brief;

(c) no person or entity other than the amici curiae contributed money that was intended to fund preparing or submitting a brief; and

(d) counsel has not represented any party in this case or in proceedings involving similar issues, or any party in a case or legal transaction at issue in the present appeal.

## STATEMENT OF INTERESTS OF AMICI

The ACLU of Massachusetts, Inc., an affiliate of the national ACLU, is a statewide nonprofit membership organization dedicated to the principle of liberty and equality embodied in the constitutions and laws of the Commonwealth and the United States. The rights they defend through direct representation and amicus briefs include the right to be free from unreasonable searches and seizures. *See, e.g., Commonwealth v. Evelyn*, SJC-12808 (2020) (amicus); *Commonwealth v. Almonor*, 482 Mass. 35 (2019) (amicus); *Commonwealth v. Augustine*, 467 Mass. 230 (2014) (direct representation); *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (direct representation).

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that works to ensure technology supports freedom, justice, and innovation for all the people of the world. For 30 years, EFF has represented technology users' interests in court cases and broader policy debates. EFF has served as amicus in numerous cases addressing Fourth Amendment protections in the digital age, including *Augustine*, 467 Mass. 230; *Carpenter*, 138 S. Ct. 2206; and *Riley v. California*, 573 U.S. 373 (2014).

## INTRODUCTION

Less than four years ago, in *Commonwealth v. White*, the Court held that a police detective's opinion that a cell phone was likely to contain evidence did not establish probable cause to search the phone, absent a "substantial basis" for concluding that the phone contained evidence of the crime under investigation. 475 Mass. 583, 588-89 (2016). Even a "[s]trong reason to suspect is not adequate," the Court explained, nor is "probable cause to suspect the defendant of a crime." *Id.* at 589, 590. Rather, "police may not seize or search [a] cellular telephone to look for evidence unless they have information establishing the existence of particularized evidence likely to be found there." *Id.* at 590-91.

But there will always be *some* facts whenever the police arrest someone with a cell phone. And particularly when the arrestee has been charged with a serious offense, law enforcement will be tempted to say those facts, whatever they are, pass the *White* test and justify a warrant to search that phone. The inevitable attempts to distinguish *White* will, in turn, risk weakening this Court's holding in that case and, with it, the constitutionally protected privacy rights of people who use cell phones.

That risk is present here. Defendant Dondre Snow is accused of participating in a murder with Dwayne Diggs.

Snow was the driver of the vehicle in which Diggs was found after Diggs shot and killed the victim. Snow had a cell phone. At the time of his arrest, he used that phone to call his girlfriend who had a possessory interest in the car he was driving so that she could retrieve the car rather than have the police tow it. Snow's cell phone was seized by police incident to his arrest. The victim's cell phone was recovered at the scene of the shooting. On the victim's cell phone were threatening messages from Diggs; there were none from Snow. Based on this information, eighty days after Snow's phone was seized, the police obtained a warrant to search it. The motion judge suppressed the evidence from that search, but a divided panel of the Appeals Court reversed the suppression order.

The Commonwealth now argues that the search passed the *White* test, based on evidence showing little more than defendant's propinquity to another who has committed a crime and his possession of a cell phone. This argument, if accepted, could undermine *White*, weaken privacy interests of cell phone users protected by the Fourth Amendment to the U.S. Constitution and Article 14 of the Massachusetts Declarations of Rights, and take the Commonwealth closer to a rule that would permit the police to search the cell phone of virtually every person arrested for a crime.

It is fitting that the Commonwealth appears to hope that this case, *Snow*, will turn out differently than the last case, *White*. In the fairy tale *Snow White*, the Queen asks a question again and again to the "mirror, mirror on the wall," hoping for a desired answer. But in court, repeating the same question should yield the same answer. The Court struck the correct balance in *White*. It should maintain that balance here in *Snow* and decline the Commonwealth's invitation to rely on insubstantial facts to establish probable cause to search a phone.

#### **STATEMENTS OF THE FACTS AND CASE<sup>1</sup>**

On the night of December 5, 2015, a person was shot multiple times in South Boston. R. 56. The shooter, later identified as Dwayne Diggs, was seen getting into a car which sped away and ultimately parked on a dead-end street two miles away from the scene of the shooting. R. 56-57, 60. The car was later found to be driven by Dondre Snow. R. 58. A third person, Daquan Peters, was also in the car. *Id.*

Police were alerted to the presence of the vehicle by an emergency call. R. 57. Police responded to the call and arrested each of the car's occupants. R. 57-58. At the time of the arrest, Snow was talking on his cell phone to his girlfriend, who had rented the vehicle

---

<sup>1</sup> "(CA.\_)" herein refers to the Commonwealth's record appendix. "(R.\_)" herein refers to the defendant-appellee's record appendix.

he was driving, to inform her of the arrest. R. 58, 59. Snow and Diggs both wore Electronic Monitoring bracelets on their ankles. R. 61.

Snow was later indicted for murder, possessing a firearm without a license, possessing ammunition without an FID card, and carrying a loaded firearm without a license. CA. 3-8. When police arrested Snow, they did what is, today, commonplace: they seized his cell phone incident to arrest. But, uncommonly, police waited nearly 80 days before seeking a warrant to search the phone. R. 62, ¶ 23.

The warrant affidavit relied primarily on three facts to assert probable cause: (1) that Snow was talking on his phone shortly before his arrest, CA. 28, ¶ 8; (2) that an alleged co-venturer, Diggs, had previously sent threatening messages to the victim, CA. 32, ¶¶ 22-23; and (3) that, given the suspected coordination of the alleged offense, CA. 34, ¶ 30, evidence of the crime likely existed on the phone.

The affidavit states, "[T]here is probable cause to believe that a cellular phone that contains communications with others, in the time before and immediately after the incident . . . may lead to relevant evidence of intent, motive and may provide additional answers as to the facts and circumstances." R. 64. It further averred that "there is probable cause to believe that photographs and contacts contained within the

target phone may lead to the identity of other potential witnesses." *Id.* And it seeks permission to search a wide swath of data "[d]ue to the fact that it is unknown as to when the weapon was acquired and when any related conspiracy may have been formed." *Id.*

The warrant was granted, and it authorized police to search nearly every conceivable aspect of the phone, including:

Cellular telephone number; electronic serial number, international mobile equipment identity, mobile equipment identifier or other similar identification number; address book; contact list; personal calendar, date book entries, and to-do lists; saved, opened, unopened, draft, sent, and deleted electronic mail; incoming, outgoing, draft, and deleted text messages and video messages; history of calls sent, received, and missed; any voicemail messages, including those that are opened, unopened, saved, or deleted; any photographs or videos, including those stored, saved, or deleted; any audio or video 'memos' stored, saved, or deleted; GPS information; mobile instant message chat logs, data and contact information; Internet browser history; and any and all of the fruits or instrumentalities of the crime of [m]urder.

CA. 23.

After his first trial ended in a mistrial, R. 46-47, the Commonwealth indicated, for the first time, that, in the second trial, it intended to introduce evidence obtained from the search of his cell phone. Snow filed a motion to suppress. R. 48.

The trial court allowed Snow's motion. R. 90. The court determined that the affidavit in support of the warrant to search Snow's cell phone failed to "establish the requisite nexus between" the murder and Snow's cell phone; "it does not establish the existence of some particularized evidence related to the crime likely to be found" on the cell phone; "and therefore, does not establish probable cause to search the defendant's cellular telephone." R. 90.

A divided Appeals Court reversed. R. 1-32. In doing so, the court relied on three factors: (1) an inference that the shooting, which was allegedly committed by two people wearing GPS tracking anklets, required planning and coordination, (2) Snow's cell phone was in the car, and he spoke with his girlfriend, whose car he drove, using that phone at the time of his arrest, and (3) Diggs exchanged violent text messages with the victim. R. 13-15.

Snow filed for further appellate review and, on April 17, 2020, this Court allowed the application. On April 22, this Court solicited the participation of amici. CA. 92.

## SUMMARY OF ARGUMENT

Consistent with this Court's decision in *White*, probable cause to search a cell phone does not arise from: (1) a person's possession and unrelated use of a cell phone at the time of their arrest and (2) an assumption that because people often communicate through cell phones, alleged co-venturers likewise communicated through cell phones. For the following reasons, a contrary conclusion would foster precisely the problems that the Court sought to avoid when it decided *White*, namely unwarranted and frequent invasions of the most private aspects of a person's life.

I. As the Supreme Court, this Court, and other courts have repeatedly recognized, cell phones contain vast amounts of sensitive information about users. Cell phones are uniquely important especially now—both in light of the ongoing global pandemic and the role cell phones have played in documenting police violence and coordinating protests against that violence, and are deserving of stringent privacy protections. (pp 11-16).

II. Because cell phones contain vast amounts of sensitive data, the U.S. Supreme Court held in *Riley* that police must obtain a warrant based on probable cause before searching a cell phone. And this Court held in *White* that police must have a substantial basis to believe that particularized evidence related to the crime under investigation exists on the phone to be

searched. *White* further held that neither an officer's training and experience nor probable cause to believe that a person participated in a crime are sufficient to establish the requisite nexus. (pp 17-20).

III. This Court should reaffirm the *White* test and the considerations that caused the Court to adopt it. Endorsing the Commonwealth's approach, and allowing proximity to a crime combined with unrelated use of a cell phone to justify a finding of probable cause, could license invasions of privacy in many cases. (pp 21-31).

#### **ARGUMENT**

**I. Cell phones are ubiquitous features of everyday life, with the capacity to store vast amounts of personal data.**

This Court has repeatedly recognized that individuals have "significant privacy interests at stake in their cellular phones and that the probable cause requirement under both the Fourth Amendment and art. 14 must serve to protect these interests." *White*, 475 Mass. at 592 (quoting *Commonwealth v. Dorelas*, 473 Mass. 496, 502 n. 11 (2016)). Among myriad other uses, phones have become essential tools used for exercising First Amendment rights, documenting law enforcement abuses and governmental overreach, and communicating with doctors, teachers, and loved ones—especially during the ongoing COVID-19 pandemic.

**A. Cell phones contain a vast amount of private data about their users.**

Ninety-six percent of American adults own a cell phone, with 81 percent owning a smartphone.<sup>2</sup> For younger people that number is even higher; 93% of people between ages 23 to 38 now own smartphones.<sup>3</sup> "Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception." *Riley v. U.S.*, 573 U.S. 373, 395 (2014).

The Supreme Court recognized in *Riley* that cell phones are distinct from physical objects and containers in both quantitative and qualitative respects. Quantitatively, the sheer volume of information available on cell phones makes them fundamentally different from any pre-digital counterpart. With their "immense storage capacity," cell phones and other electronic devices can contain the equivalent of "millions of pages of text, thousands of pictures, or

---

<sup>2</sup> Pew Research Center, *Mobile Fact Sheet* (June 12, 2019), <http://www.pewinternet.org/fact-sheet/mobile/>. Cf. *Riley*, 573 U.S. at 385 (citing A. Smith, Pew Research Center, *Smartphone Ownership—2013 Update* (June 5, 2013) (noting "56% of American adults are now smartphone owners"))).

<sup>3</sup> Emily A. Vogels, *Millennials stand out for their technology use, but older generations also embrace digital life*, Pew Research Center (Sept. 9, 2019), <https://pewresearch-org-preprod.go-vip.co/fact-tank/2019/09/09/us-generations-technology-use/>.

hundreds of videos." *Id.* at 393, 394. The storage capacity of the average smartphone today—at over 80 gigabytes<sup>4</sup>—is five times as large as when *Riley* was decided just six years ago. See *id.* at 394 (16 gigabytes). The storage capacity of phones, and thus the quantity of personal information they contain, will only continue to increase.<sup>5</sup>

Qualitatively, cell phones "collect[] in one place many distinct types of information . . . that reveal much more in combination than any isolated record." *Riley*, 573 U.S. at 394. Average smartphone users now have 60-90 different apps on their devices and use 30 different apps per month.<sup>6</sup> Apps generate vast and varied data, including call logs, emails, text messages, voicemails, browsing history, calendar entries, contact lists, shopping lists, notes, photos and videos, books read, TV shows and movies watched, financial and health data, purchase history, dating profiles, metadata, and

---

<sup>4</sup> Sujeong Lim, *Average Storage Capacity in Smartphones to Cross 80GB by End-2019*, Counterpoint (Mar. 16, 2019), <https://www.counterpointresearch.com/average-storage-capacity-smartphones-cross-80gb-end-2019>.

<sup>5</sup> Lim, *supra* note 4.

<sup>6</sup> See *Riley*, 573 U.S. at 396 (describing various apps and noting, at that time, that the average smartphone user "has installed 33 apps, which together can form a revealing montage of the user's life."); Sarah Perez, *Report: Smartphone owners are using 9 apps per day, 30 per month*, TechCrunch (May 4, 2017), <https://techcrunch.com/2017/05/04/report-smartphone-owners-are-using-9-apps-per-day-30-per-month>.

so much more. This information, in turn, can reveal an individual's political affiliations, religious beliefs and practices, sexual and romantic life, financial status, health conditions, and family and professional associations. *See id.* at 394-96.

The ability of cell phones to access data that is not stored on the phone itself but in the "cloud," *i.e.*, on a server elsewhere, "further complicate[s] the scope of the privacy interest at stake." *Riley*, 573 U.S. at 397. "Virtually any digital action that internet users may take—from using credit cards to logging into social media sites—creates data that is stored by companies, governments or other organizations."<sup>7</sup> Although the information stored in the cloud should not be accessed by law enforcement who are searching through a phone, "officers searching a phone's data would not typically know whether the information they are viewing was stored locally . . . or has been pulled from the cloud." *Riley*, 573 U.S. at 397.

**B. Cell phones are unique tools for exercising constitutional rights and conducting private communications.**

Cell phones play an indispensable role in the modern world, especially in facilitating the exercise of

---

<sup>7</sup> Aaron Smith, *Americans' experiences with data security*, Pew Research Center (Jan. 26, 2017), <https://www.pewresearch.org/internet/2017/01/26/1-americans-experiences-with-data-security>.

people's First Amendment rights to association and expression.

Today, it is the rare newsworthy event that is not captured on a cell phone video, notably including incidents of official misconduct and police brutality. *See, e.g., Glik v. Cunniffe*, 655 F.3d 78, 79 (1st Cir. 2011) (First Amendment protected individual who used cell phone to record police conduct in public). And when these cell phone videos spur widespread protest—as with the unprecedented response to the video-recorded killing of George Floyd by Minneapolis police officers—individuals use their phones to coordinate marches, demonstrations, and collective action.

Phones are also central to the privacy of modern communications, particularly for those who use their phones as a primary or even sole means of connecting to the Internet. In 2019, 17% of Americans were “mobile dependent,” meaning they owned a smartphone but did not have a home broadband connection.<sup>8</sup> The people in this group were more likely to be young, Black or Hispanic, and lower-income.<sup>9</sup> And Black and Hispanic people were accordingly found more likely than whites to rely on

---

<sup>8</sup> Pew Research Center, *Mobile Fact Sheet*, *supra* note 2.

<sup>9</sup> *Id.*

their smartphones for a number of activities such as seeking health information or looking for work.<sup>10</sup>

The ongoing COVID-19 pandemic has further increased the use of technology to communicate, as many conversations that might have otherwise been face-to-face are now conducted through FaceTime or Zoom. Children attend school, doctors treat patients,<sup>11</sup> and family, friends, and lovers meet—all online and frequently on a mobile device. Roughly 76% of Americans are estimated to be using email or messaging services to communicate with others during the pandemic, while 70% have searched online for health information about the coronavirus.<sup>12</sup>

As a result of the COVID-19 crisis, the data on our phones reveals even more, and even more private, information about our lives.

---

<sup>10</sup> Andrew Perrin and Erica Turner, *Smartphones help blacks, Hispanics bridge some - but not all - digital gaps with whites*, Pew Research Center (Aug. 20, 2019), <https://www.pewresearch.org/fact-tank/2019/08/20/smartphones-help-blacks-hispanics-bridge-some-but-not-all-digital-gaps-with-whites/>.

<sup>11</sup> *US Virtual Care Visits To Soar To More Than 1 Billion*, Forrester (Apr. 10, 2020) <https://go.forrester.com/press-newsroom/us-virtual-care-visits-to-soar-to-more-than-1-billion/>.

<sup>12</sup> Monica Anderson & Emily A. Vogels, *Americans turn to technology during COVID-19 outbreak*, Pew Research Center (March 31, 2020), <https://www.pewresearch.org/fact-tank/2020/03/31/americans-turn-to-technology-during-covid-19-outbreak-say-an-outage-would-be-a-problem/>.

**II. This Court has determined that the vast storage and communications capacities of cell phones cannot automatically establish probable cause to search and seize a person's cell phone.**

Decisions by the Supreme Court and this Court make clear that the vast quantities of private information stored on cell phones supply a reason to enforce, rather than ease, constitutional protections that stand between that information and law enforcement. In *Riley*, 573 U.S. at 394, the Supreme Court recognized that cell phones can reconstruct an individual's life, and the Court therefore held that the Fourth Amendment does not permit police to conduct a warrantless search of a cell phone incident to arrest. In *Dorelas*, this Court explained that, due to a cell phone's "distinct" qualities, a search of its many files must be done with special care" and "satisfy a more narrow and demanding standard." 473 Mass. at 502. And in *White*, this Court concluded that before a cell phone can be searched, Article 14 and the Fourth Amendment require probable cause that "some particularized evidence related to the crime" exists on the phone. 475 Mass. at 589 (internal quotations omitted). The decision in this case should follow that same approach.

**A. The Supreme Court has limited searches of cell phones incident to arrest because they contain vast, private, and sensitive information.**

Although it did not involve the precise legal issues presented here, the Supreme Court's decision in

*Riley*, concerning warrantless searches of cell phones incident to arrest, can inform this Court's decision-making about the quantum of evidence that police must demonstrate in order to obtain a warrant to search the phone of an arrestee. *Riley* turned, in significant part, on the fact that cell phones have become so central to daily life "that the proverbial visitor from Mars might conclude they were an important feature of human anatomy." 573 U.S. at 385. Cell phones are "not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans 'the privacies of life.'" *Id.* at 403. (quoting *Boyd v. U.S.*, 116 U.S. 616, 630 (1886)).

The Supreme Court's fundamental conclusion in *Riley*, that police must "get a warrant" to search the phone of an arrestee, would mean very little if the ability to obtain a warrant was an automatic consequence of making an arrest. That cell phones are capable of holding tremendous amounts of information is a reason to require a meaningful showing of probable cause; it is not a reason to say that probable cause has been established by the arrestee's use of the phone. *Cf. id.* at 386; *Commonwealth v. Augustine*, 472 Mass. 448, 455 (2015).

**B. *White* requires probable cause to believe that particularized evidence related to the crime under investigation exists on the cell phone.**

In *White*, a police detective seized the cell phone of a person suspected to have participated in an armed robbery and shooting. 475 Mass. at 586. At the time of the seizure, which preceded the defendant's arrest, police had information from the defendant's mother about defendant's involvement in the robbery and, from a consent search of the defendant's bedroom, had retrieved a jacket similar to one worn by one of the perpetrators. *Id.* at 585. What police did not have was "any information that a cell phone was used in the" robbery and shooting, "nor did they claim that there existed a particular piece of evidence likely to found on such a device." *Id.* at 590 (internal marks omitted). Instead, "they were aware, based on their experience, that such devices often contained useful information in cases involving multiple perpetrators." *Id.* at 586.

The Court held that police lacked probable cause to seize the phone. *Id.* at 592. In doing so, the Court established that police may not base probable cause determinations solely on: (1) the existence of evidence that multiple people participated in a crime; and (2) the belief, based on officers' training and experience, that "if the defendant planned and committed [the crime] with two coventurers, it was likely he did so, at least in part using his cellular telephone," and that,

therefore, his cell phone will likely contain communications with his co-venturers. *Id.* at 590, 591. “[S]uch considerations ‘do not, alone, furnish the requisite nexus between the criminal activity and the places to be searched’ or seized.” *Id.* at 591 (quoting *Commonwealth v. Anthony*, 451 Mass. 59, 72 (2008)).

There must instead be “a substantial basis” for concluding that the cell phone contains “particularized evidence” connected or related to the crime under investigation. *Id.* at 588-89. This is so “even where there is probable cause to suspect the defendant of a crime. *Id.* at 590. “Only then . . . do [police] have probable cause to seize and search the device in pursuit of evidence.” *Id.* at 589; see also *In re Search of Certain Cell Phones*, 541 F. Supp. 2d 1, 2 (D.D.C. 2008) (holding that, to establish probable cause, there must be some specific and objective “indication that the [cell phone] owner ever used the phone” in relation to the crime); see also *People v. Taylor*, 2002 WL 465094, at \*16 (N.Y. Sup. Ct. Mar. 20, 2002) (holding a probable cause justification was merely “speculative” where police inferred from the defendant’s use of his phone that he may have also used it “for other similar purposes” in relation to the crime).

**III. This Court should reaffirm *White's* holding that police need particularized evidence connecting the cell phone to be searched with the crime under investigation.**

The Commonwealth's arguments, in effect, ask this Court to weaken its decision in *White*. The Court should not do so, lest it license significant invasions of privacy based on nothing more than someone's use of a phone while physically proximate to someone involved in a crime.

**A. Mere presence and use of a cell phone at the scene of an arrest fails to establish probable cause to search the device.**

Probable cause requires a nexus between the crime under investigation and the cell phone to be searched. *White*, 475 Mass. at 588. Precisely because cell phones are such an integral part of modern life, it will almost always be possible for the Commonwealth to hypothesize that an arrestee may have used his phone to commit the crime under investigation. But the Commonwealth's argument in this case fails to demonstrate the nexus that *White* requires, even when considering all reasonable inferences which may be drawn from the information in the warrant affidavit.

The Commonwealth argues that because (1) a passenger in Snow's car was suspected of having committed a crime and had previously communicated with the victim; (2) there were three people in the car "each of whom had a cell phone with him inside the vehicle";

and (3) Snow spoke with his girlfriend at the time of his arrest<sup>13</sup> in order to apprise her of the arrest itself, the police could infer that his cell phone would contain evidence linking him to the crime. See Com. Br. at 21, 24, 26, 31-32.

First, it is unclear how communications between *Diggs* and the victim, combined with the presence of *Diggs* in Snow's car after the murder, establish a nexus between Snow's phone and the crime. Probable cause to search someone's cell phone seems unlikely to arise from how an acquaintance of that person has chosen to use their cell phone. *Cf. Commonwealth v. Morin*, 478 Mass. 415, 426 (2017) ("information that an individual communicated with another person, who may have been linked to a crime, without more, is insufficient to establish probable cause to search either individual's cellular telephone"); *Buckham v. State*, 185 A.3d 1, 17 (Del. 2018) ("Particularly unpersuasive was the statement that 'criminals often communicate through cellular phones' (who doesn't in this day and age?) and the statement that Waters' girlfriend—who owns the vehicle that Waters was allegedly driving on the day of the shooting—'contacted Buckham's girlfriend via cell phone' before she spoke with the police about the incident, which

---

<sup>13</sup> *Amici* read the record as suggesting only that Snow was talking on his cell phone when it became clear that he was about to be arrested. Com. Br. at 11, 13.

provides no basis at all to suspect that Buckham's cell phone was likely to contain evidence." ).

Second, probable cause to search a phone cannot be said to arise from the fact that the crime under investigation may have involved multiple perpetrators. *Morin*, 478 Mass. at 426 ("police may not rely on the general ubiquitous presence of cellular telephones in daily life, or an inference that friends or associates most often communicate by cellular telephone, as a substitute for particularized information that a specific device contains evidence of a crime"). As applied here, the fact that Snow, Diggs, and Peters were in a car and, like 96% of American adults, they each had a cell phone would not establish probable cause to believe that they communicated using their cell phones to plan a murder. See *Commonwealth v. Jordan*, 91 Mass. App. Ct. 743, 750 (2017) (to establish probable cause to retrieve data from a cell phone, it is not enough to rely on "generalities that friends or coventurers often use cellular telephones to communicate"). Importantly, the Commonwealth has presented no evidence to suggest, and nothing in the record supports a finding, that this murder was either planned or coordinated, let alone planned or coordinated through cell phone communications. See Com. Br. At 40-43; compare *Commonwealth v. Holley*, 478 Mass. 508, 526 (2017) (defendants, who lived separately, arrived at victim's

house at the same time and were both seen on their cell phones); *Commonwealth v. Arthur*, 94 Mass. App. Ct. 161, 165 (2018) (co-venturers arrived together in two separate cars and left their vehicles in sequence while leaving the engine running).

Instead, the Commonwealth attempts to argue that probable cause exists because the police believed that *if* these three individuals *had* planned and committed the murder, it was likely they had communicated by using their cell phones, and accordingly, likely that evidence of these communications would be found on the device. Com. Br. at 31-32; *see also* R. 64 (warrant affidavit).

This same argument was rejected by the Court in *White*. 475 Mass. at 590. As the Court explained there, the mere possibility that a person could keep on their cell phone a digital record of communications with their co-venturers, without more, is not enough to establish probable cause. *Id.* at 591; *see also* *Commonwealth v. Broom*, 474 Mass. 486, 496-497 (2016) (“general” and “conclusory” opinion by affiant that individual is likely to store information in cell phone does not satisfy probable cause standard).

Third, an arrestee’s use of a cell phone at the time of arrest, especially without proof that he used the phone at any time during the commission of the alleged crime, cannot satisfy probable cause. Therefore, that Snow called his girlfriend to apprise her of his

arrest so that she may retrieve her car does not establish probable cause.<sup>14</sup> See *Buckham*, 185 A.3d at 17 (“the fact that [defendant] may have been using his phone to talk about his impending arrest connects his phone to the arrest warrant, not the underlying crime.”); see also *Jordan*, 91 Mass. App. Ct. at 750-51 (declining to find probable cause based on evidence that defendant called two family members around the time of the murder). As Judge Henry wrote in dissenting from the Appeals Court’s decision, the logic of the Commonwealth’s argument is that “although the ubiquity of cell phones cannot justify a search, if a person actually uses rather than just carries that cell phone shortly after committing a crime, then the cell phone is probably connected to the crime and subject to search.” *Commonwealth v. Snow*, 96 Mass. App. Ct. 672, 681 (2019) (Henry, J. dissenting in part, concurring in part). The Commonwealth’s logic would justify a finding of probable cause anytime it can be shown that a person suspected of a crime used their cell phone, for any reason, in close

---

<sup>14</sup> Although the Commonwealth argues that Snow “was trying to ensure that the car used in the shooting did not remain in police custody,” Com. Br. at 23, the warrant affidavit clearly states that the police had already conducted a search of the vehicle (with the consent of Snow’s girlfriend) and found no evidence to support an inference that the vehicle would need to be hidden in order to destroy evidence. R. 59.

temporal proximity to the commission of a crime.<sup>15</sup> This will presumably be an easy showing given that, for many people, cell phone use is constant.

In short, "the affidavit made no connection between the defendant's use of his cellular telephone and his involvement in the crime." See *Jordan*, 91 Mass. App. Ct. at 751. This is insufficient to establish probable cause under *White*.

**B. The Commonwealth's inability to identify a timeframe or location for any alleged evidence on the phone further underscores their lack of probable cause.**

The absence of probable cause to search Snow's cell phone is also reflected in the boundless scope of the requested search. Search warrants must clearly define and limit the scope of the search. *Commonwealth v. Pope*, 354 Mass. 625, 629 (1968). The particularity requirement protects individuals from the general searches allowed under the "reviled 'general warrants' and 'writs of

---

<sup>15</sup> In fact, this Court recently held in *Commonwealth v. Goncalves-Mendez*, that it is "the better practice" for police to inform an individual, prior to seizing his car upon arrest, "that the vehicle will be taken to a police facility or private storage facility for safekeeping unless the driver directs the officer to dispose of it in some lawful manner." 484 Mass. 80, 85 n.8 (2020). Snow telephoned his girlfriend, who had lawful possessory interest in the car, so that she may retain custody of the vehicle rather than have the police tow it. Yet, here, Snow's exercise of his art. 14 rights is being proffered as evidence of criminality. Com. Br. at 23.

assistance' of the colonial era." *Riley*, 373 U.S. at 403.

Despite this requirement, the Boston Police Department submitted a warrant application on February 23, 2016, more than 80 days after having seized Snow's cell phone, to search virtually all data on the phone "without date restriction." R. 52, 64. This unfettered search was requested, it seems, not because the BPD had evidence of the requisite nexus between the crime alleged and the cell phone to be searched, see R. 64-65, but precisely because the BPD lacked such evidence. The warrant application could not say where incriminating evidence could be expected to be found on the cell phone because law enforcement lacked evidence to suggest there was a conspiracy between Snow and Diggs; when such conspiracy formed (if it existed at all); and when the murder weapon was acquired (and presumably who acquired it). R. 64.

Thus, the BPD was constrained to request authorization to comb through information stored on Snow's phone, "including but not limited to" the 13 data storage locations specified in the affidavit and application as well as "any and all of the fruits or instrumentalities of the crime of Murder." R. 65. But such grasping for evidence runs directly counter to the particularity requirement, which "serves as a safeguard against general exploratory rummaging by police through

a person's belongings." *Commonwealth v. Freiberg*, 405 Mass. 282, 298 (1989). The Commonwealth's inability to specify what exactly it was searching for was a reason for the warrant application to be rejected, rather than for it to proceed without any meaningful constraint on its scope.

**C. The Commonwealth's approach threatens privacy.**

Accepting the Commonwealth's arguments in this case would risk creating the very situation that this Court sought to avoid in *White*, namely that "it would be a rare case where probable cause to charge someone with a crime would not open the person's cellular telephone to seizure and subsequent search." *White*, 475 Mass. at 591. Under the Commonwealth's approach, police could have license to search the phone of anyone who merely happens to be nearby when a crime involving more than one person is alleged to have occurred. This would have a disproportionate impact on the privacy interests of law-abiding people engaged in peaceful protest throughout the Commonwealth.

For example, the country has been experiencing nationwide protests against police brutality in the wake of George Floyd's death at the knee of a police officer. Not only was his death-and the death of many other Black Americans-captured on cell phone, which galvanized people to take to the streets to push for police reform, but the activities of police in response to those initial

protests were captured on cell phone as well. These cell phone videos opened the eyes of even more Americans and people around the world to the indignities police perpetrate on communities of color every day. None of these events could have been recorded if not for the fact that these protestors took their phones to and used them at the protests.

However, by early June, in response to these protests, police across the country had arrested over 10,000 people, many for low-level offenses such as curfew violation or failure to disperse.<sup>16</sup> In Boston, 11 people were arrested solely on charges of disorderly conduct and/or disturbing the peace following the protest on May 31.<sup>17</sup> As a matter of routine during mass arrests, police seized cell phones and other personal possessions incident to arrest,<sup>18</sup> even though many cities

---

<sup>16</sup> Anita Snow, *AP tally: Arrests at widespread US protests hit 10,000*, AP (June 4, 2020), <https://apnews.com/bb2404f9b13c8b53b94c73f818f6a0b7>.

<sup>17</sup> BPD News, *BPD Confirms Fifty-Three Arrests Made and One Summons Issued Following Protests in Boston* (June 1, 2020), <https://bpdnews.com/news/2020/6/1/bpd-confirms-fifty-three-arrests-made-and-one-summons-issued-following-protests-in-boston>.

<sup>18</sup> Samantha Fields, *What it can cost to get arrested at a protest*, Marketplace (June 10, 2020), <https://www.marketplace.org/2020/06/10/what-it-can-cost-to-get-arrested-at-a-protest/>.

quickly dropped or reduced charges against many of the arrestees.<sup>19</sup>

But if the Commonwealth's arguments prevail, arrests like these during political protests could potentially furnish police with everything they need to search seized phones. Many people bring phones to document protests; they may well be in the process of using a phone during an arrest (perhaps even to document the arrest itself); and they are standing amongst many other individuals engaged in similar protest activities. For example, during protests police frequently invoke crimes such as incitement to riot, which under both Massachusetts and federal law involve the participation of several people. See, e.g., Mass. Gen. Laws ch. 269 §§ 1-2; 18 U.S.C. § 2102(b). Such a charge—even if dropped days later—could suggest “evidence of

---

<sup>19</sup> Bill Chappell, *Fort Worth Police Drop Rioting Charges Against Protesters*, NPR (June 9, 2020), <https://www.npr.org/sections/live-updates-protests-for-racial-justice/2020/06/09/872827789/fort-worth-police-drop-rioting-charges-against-protesters-topic-of-a-broad-debat>; Whitney Woodworth, *Criminal charges dismissed against 14 arrested at Black Lives Matter protests*, Statesman Journal (June 29, 2020), <https://www.statesmanjournal.com/story/news/crime/2020/06/29/charges-dropped-black-lives-matter-salem-oregon-protests/3283065001/>; Ryan Deto, *Pittsburgh's first two BLM protests led to dozens of arrests; about 90% of those charges have been dropped*, Pittsburgh City Paper (June 19, 2020), <https://www.pghcitypaper.com/pittsburgh/pittsburghs-first-two-blm-protests-led-to-dozens-of-arrests-about-90-of-those-charges-have-been-dropped/Content?oid=17489183>.

coordination" sufficient under the Commonwealth's reasoning to provide probable cause to search a seized phone.

The Fourth Amendment prohibits searches of individuals based on a "mere propinquity to others independently suspected of criminal activity." *Ybarra v. Illinois*, 444 U.S. 85, 91 (1979). The need for independent probable cause to search a person is grounded in the important interest in "safeguarding citizens from rash and unreasonable interferences with privacy." *Id.* at 95-96 (citations omitted). Searches of cell phones should be no different, but the Commonwealth seeks to undermine that bedrock rule here.

Whether a person is arrested at a large protest or suspected of coordinating illegal acts with other occupants of a car, the mere propinquity of a cell phone to that activity does not constitute probable cause to search that device.

#### **CONCLUSION**

*Amici* respectfully ask the Court to affirm the *White* test and require a strict adherence to the requirement that, in seeking to establish probable cause to search a cell phone, the Commonwealth must establish a substantial basis for asserting that the phone contains evidence of a crime.

Respectfully submitted,

/s/ Mark Rumold  
Jennifer Lynch (CA 240701)  
Andrew Crocker (CA 291596)  
Mark Rumold (CA 279060)  
Hannah Zhao (NY 5468673)  
ELECTRONIC FRONTIER FOUNDATION  
815 Eddy Street  
San Francisco, CA 94109  
(415) 436-9333  
jlynch@eff.org

/s/ Jessica J. Lewis  
Matthew R. Segal, BBO #654489  
Jessie J. Rossman (BBO 670685)  
Jessica J. Lewis, BBO #704229  
AMERICAN CIVIL LIBERTIES UNION  
FOUNDATION OF MASSACHUSETTS, INC.  
211 Congress Street  
Boston, MA 02110  
(617) 482-3170  
jlewis@aclum.org

Counsel for *Amici Curiae*

**CERTIFICATE OF COMPLIANCE**

I, Jessica Lewis, hereby certify that this brief complies with the rules of court pertaining to the filing of briefs, including, but not limited to: Mass. R. App. P. 16(a)(6) (pertinent findings or memorandum of decision); Mass. R. App. P. 16(e) (references to the record); Mass. R. App. P. 16(f) (reproduction of statutes, rules, regulations); Mass. R. App. P. 16(h) (length of briefs); Mass. R. App. P. 18 (appendix to the briefs); and Mass. R. App. P. 20 (form of briefs, appendices, and other papers).

/s/ Jessica J. Lewis  
Jessica J. Lewis

**AFFIDAVIT OF SERVICE**

I, Jessica J. Lewis, counsel for the American Civil Liberties Union of Massachusetts, Inc. do hereby certify under the penalties of perjury that on this 28th day of August, 2020, I caused a true copy of the foregoing document to be served by electronic filing through the CM/ECF system on the following counsel and that paper copies will be sent to any non-registered participants:

Cailin M. Campbell  
Chief of Appeals  
Assistant District Attorney  
for the Suffolk District  
One Bulfinch Pl.  
Boston, MA 02114  
cailin.campbell@state.ma.us  
Counsel for the  
Commonwealth

Amy M. Belger  
Law Office of Amy M.  
Belger  
841 Washington Street  
Holliston, MA 01746  
appellatedefender@gmail.  
com  
Counsel for Defendant-  
Appellee Dondre Snow

/s/ Jessica J. Lewis  
Jessica J. Lewis

No. SJC-12938

---

Commonwealth of Massachusetts  
Appellant

v.

Dondre Snow,  
Defendant-Appellee.

---

ON APPEAL FROM A JUDGMENT OF  
THE SUFFOLK SUPERIOR COURT

---

**BRIEF AMICI CURIAE OF THE AMERICAN CIVIL LIBERTIES  
UNION OF MASSACHUSETTS, INC. AND THE ELECTRONIC  
FRONTIER FOUNDATION IN SUPPORT OF THE APPELLEE**

---

NOTICE: All slip opinions and orders are subject to formal revision and are superseded by the advance sheets and bound volumes of the Official Reports. If you find a typographical error or other formal error, please notify the Reporter of Decisions, Supreme Judicial Court, John Adams Courthouse, 1 Pemberton Square, Suite 2500, Boston, MA, 02108-1750; (617) 557-1030; SJCRReporter@sjc.state.ma.us

SJC-12938

COMMONWEALTH vs. DONDRE SNOW.

Suffolk. September 11, 2020. - January 11, 2021.

Present: Lenk, Gaziano, Lowy, Budd, Cypher, & Kafker, JJ.<sup>1</sup>

Homicide. Firearms. Cellular Telephone. Constitutional Law,  
Search and seizure, Probable cause. Search and Seizure,  
Probable cause. Probable Cause. Practice, Criminal,  
Motion to suppress.

Indictments found and returned in the Superior Court Department on February 26, 2016.

A pretrial motion to suppress evidence was heard by Maureen B. Hogan, J.

An application for leave to prosecute an interlocutory appeal was allowed by Gants, C.J., in the Supreme Judicial Court for the county of Suffolk, and the appeal was reported by him to the Appeals Court. After review by the Appeals Court, the Supreme Judicial Court granted leave to obtain further appellate review.

Cailin M. Campbell, Assistant District Attorney (David D. McGowan, Assistant District Attorney, also present) for the Commonwealth.

Amy M. Belger for the defendant.

---

<sup>1</sup> Justice Lenk participated in the deliberation on this case prior to her retirement.

Jennifer Lynch, Andrew Crocker, & Mark Rumold, of California, Hannah Zhao, of New York, Matthew R. Segal, Jessie J. Rossman, & Jessica J. Lewis, for American Civil Liberties Union of Massachusetts, Inc., & another, amici curiae, submitted a brief.

LOWY, J. On the night of December 5, 2015, the defendant, Dondre Snow, and two other men were arrested in connection with a fatal shooting that had occurred earlier that evening in Boston. Police officers seized the defendant's cell phone, and a police detective later applied for and received a search warrant to search it for evidence related to the crime. Before trial, the Commonwealth moved to introduce certain evidence found on the defendant's cell phone. The defendant moved to suppress the cell phone evidence. The judge allowed the defendant's motion, ruling that the warrant had issued without probable cause because it lacked a sufficient nexus between the murder and the defendant's cell phone. Although the judge did not explicitly rule on whether the search authorized by the warrant was sufficiently particular, she apparently factored it into her analysis, noting at the hearing that the search was not limited in time.

The Commonwealth filed an application for interlocutory review in the county court, which a single justice of this court allowed and reported to the Appeals Court. The Appeals Court, in a divided opinion, reversed the judge's decision and remanded

for a determination whether the warrant was properly limited in scope. The matter was entered in this court following our grant of further appellate review.

We consider, first, whether there was probable cause to search the defendant's cell phone and, second, whether the search exceeded the permissible scope of the warrant. We conclude there was probable cause to search the defendant's cell phone, based on the defendant's cell phone call shortly after the crime had been committed to the person who had rented the getaway car, as well as on the inference that the joint venture crime was planned ahead of time. We also conclude that the search of the phone was not sufficiently particular because it lacked any temporal limit. The order allowing the defendant's motion to suppress is vacated, and we remand to the Superior Court for further rulings regarding partial suppression.<sup>2</sup>

1. Background. The following facts are taken from the search warrant affidavit. On the evening of December 5, 2015, Maurice Scott was shot several times as he stood on a Boston street. He later died from gunshot wounds. One eyewitness heard a number of shots fired and then saw a "heavy set black male" standing over the victim as he lay on the ground.

---

<sup>2</sup> We acknowledge the amicus brief submitted by the American Civil Liberties Union of Massachusetts, Inc., and the Electronic Frontier Foundation.

The shooter fled the scene in a light-colored car with out-of-State license plates driven by another party. During the shooting, the getaway car had been parked up the street. The car then headed toward the Dorchester neighborhood of Boston. Several minutes later, a second witness saw a light gray sedan being driven quickly down a street in Dorchester. The driver of the car slammed on its brakes, backed up, and took a left turn onto a dead-end street before coming to a stop. The witness noticed the occupants of the car moving about, as if they were changing their clothes. A large man climbed out of the passenger's seat, pulled his sweatshirt down, and returned to the car. The witness telephoned the police.

When police arrived, they noticed a light gray 2016 Nissan Altima with a New Hampshire license plate parked near the dead end of the street. Three men were sitting in the car: the defendant in the driver's seat, Dwayne Diggs in the front passenger's seat, and Daquan Peters in the back seat. Officers noted that Diggs had a heavy build and fit the eyewitness's description of the shooter. Based on the matching witness descriptions of the car used in the shooting and Diggs as the shooter, the officers removed all three men from the car. The defendant was talking on his cell phone as officers removed him from the car.

Officers discovered a .40 caliber firearm near the car and, by using thermal imaging, found that the heat signature indicated that the firearm recently had been discarded. Officers also discovered nine .40 caliber spent shell casings at the scene of the shooting. A fingerprint from the magazine of the gun matched Diggs's fingerprint. Both the defendant and Diggs were wearing global positioning system (GPS) monitors, which placed each of them at the crime scene at the time of the shooting. Police seized the defendant's cell phone, Peters's cell phone, and a third cell phone from the Nissan's center console with Diggs's partial fingerprint on it.

The defendant told officers that the car was rented to his girlfriend, and asked repeatedly during the booking process how she could get it back. The next day, police interviewed the defendant's girlfriend. She told officers that although she had a car, she had rented the Nissan to assist her with a move to Fall River. She also noted that she had rented a different car earlier in the week, but switched it for the Nissan on December 5. Finally, she told officers that the defendant had called her from his cell phone to let her know he was about to be arrested.

Officers also recovered the victim's cell phone, and a search revealed violent and threatening text messages exchanged with a contact named "Slime Buttah." Interviews with the victim's acquaintances revealed that the victim and Diggs had

been arguing via text message and social media in the days before the murder. Diggs's street names included "Butta" and "Butta Bear." Based on both of these pieces of information, detectives believed "Slime Buttah" to be Diggs.

On February 23, 2016, a detective applied for and received a warrant to search the defendant's cell phone for the following information:

"Cellular telephone number; electronic serial number, international mobile equipment identity, mobile equipment identifier or other similar identification number; address book; contact list; personal calendar, date book entries, and to-do lists; saved, opened, unopened, draft, sent, and deleted electronic mail; incoming, outgoing, draft, and deleted text messages and video messages; history of calls sent, received, and missed; any voicemail messages, including those that are opened, unopened, saved, or deleted; GPS information; mobile instant message chat logs, data and contact information; internet browser history; and any and all of the fruits or instrumentalities of the crime of Murder."

The detective requested and received permission to search unfettered by date restriction because, he said, it was unknown "when the weapon used was acquired and when any related conspiracy may have been formed."

2. Discussion. a. Probable cause. On appeal, the Commonwealth challenges the judge's ruling that the contents of the warrant affidavit failed to establish a nexus between the crime and the defendant's cell phone sufficient support a finding of probable cause to search it. The Commonwealth contends that a sufficient nexus may be derived from the

affidavit's allegations concerning the defendant's call to his girlfriend, who had rented the getaway car, the reasonable inferences of planning and coordination that may be drawn from the change of clothing, and Diggs's violent text messages to the victim. For the reasons explained infra, we agree and thus vacate the judge's order suppressing the evidence recovered from the search of the defendant's cell phone.

"Both the Fourth Amendment to the United States Constitution and art. 14 of the Massachusetts Declaration of Rights 'require a magistrate to determine that probable cause exists before issuing a search warrant.'" Commonwealth v. Holley, 478 Mass. 508, 521 (2017), quoting Commonwealth v. Cavitt, 460 Mass. 617, 626 (2011). Probable cause requires a "'substantial basis' to conclude that 'the items sought are related to the criminal activity under investigation, and that they reasonably may be expected to be located in the place to be searched at the time the search warrant issues.'" Holley, supra, quoting Commonwealth v. Kaupp, 453 Mass. 102, 110 (2009). In other words, the government must show not only that there is probable cause that the individual committed a crime but also that there is a "nexus" between the alleged crime and the article to be searched or seized. Commonwealth v. White, 475 Mass. 583, 588 (2016). The nexus does not need to be based on direct observation; it can be found in "'the type of crime, the

nature of the [evidence] sought, and normal inferences as to where such' evidence may be found" (citation omitted). Id. at 589. "While 'definitive proof' is not necessary to meet this standard, the warrant application may not be based on mere speculation," Holley, supra, quoting Commonwealth v. Augustine, 472 Mass. 448, 455 (2015), or a "[s]trong reason to suspect," Commonwealth v. Upton, 394 Mass. 363, 370 (1985).

Probable cause is a "fact-intensive inquiry and must be resolved based on the particular facts of each case." Commonwealth v. Morin, 478 Mass. 415, 426 (2017). With respect to cell phone searches, "police may not rely on the general ubiquitous presence of cellular telephones in daily life, or an inference that friends or associates most often communicate by cellular telephone, as a substitute for particularized information that a specific device contains evidence of a crime." Id. at 426.

"When considering the sufficiency of a search warrant application, our review begins and ends with the four corners of the affidavit" (quotation and citation omitted). Holley, 478 Mass. at 521. The affidavit is to be "considered as a whole and in a commonsense and realistic fashion" and should not be "parsed, severed, and subjected to hypercritical analysis." Commonwealth v. Dorelas, 473 Mass. 496, 501 (2016), quoting Commonwealth v. Donahue, 430 Mass. 710, 712 (2000). "All

reasonable inferences which may be drawn from the information in the affidavit may also be considered as to whether probable cause has been established." Holley, supra 521-522, quoting Donahue, supra.

Here, the affidavit provided a substantial basis to conclude both that the defendant had committed the homicide as Diggs's coventurer and that it was reasonable to expect that his cell phone would contain evidence related to that specific crime.<sup>3</sup> Not only was the defendant apparently calling his girlfriend to ask her to retrieve the car soon after the crime, but his girlfriend had an improbable explanation for having rented a car at all, given that she already owned one. See, e.g., United States v. Winters, 782 F.3d 289, 299-301 (6th Cir. 2015) (implausible explanation for renting car was one factor giving rise to reasonable suspicion). When she was later interviewed by police, the defendant's girlfriend asserted that, although she had a car, she had rented an extra car to assist in her move to Fall River. The rental car was a Nissan Altima -- a sedan -- not the typical truck or van one might rent for moving. Moreover, she noted that she had rented a different vehicle earlier in the week and had exchanged it for the Nissan on that day, but did not provide a reason for the change.

---

<sup>3</sup> The defendant does not dispute that the warrant contained probable cause that he committed a crime.

Additionally, when he was being booked, the defendant asked officers how his girlfriend could get her car back, and stated that he did want not to have a bill for a late fee. Given that the defendant was about to be arrested for murder, it seems unlikely that he was calling his girlfriend merely to ensure that she could pick up the rental car and avoid a charge for a late rental return. The rental car contained evidence related to the shooting: a T-shirt and a third cell phone, both of which presumably belonged to Diggs.<sup>4</sup> Given the context, it seems probable that the defendant's call was motivated by a concern that evidence could be discovered in the car, not by a possible late fee.

Finally, there was some evidence that the crime had been planned ahead of time. The search warrant affidavit noted that a witness saw "people moving around in the car leaving the impression on him that they might be changing their clothes." This leads to an inference that the crime had involved, at a minimum, enough prior planning and coordination for the parties to bring a change of clothes.<sup>5</sup> Further, the evidence that Diggs

---

<sup>4</sup> Diggs's cell phone likely would have contained evidence of communications between him and the victim, given that the victim's cell phone contained threatening text messages from "Slime Buttah," believed to be Diggs.

<sup>5</sup> A black T-shirt, size 6X, and a black sweatshirt, size large, were recovered from inside the Nissan. Given the disparity in sizes, it is likely that these items did not belong to the same person. The affidavit permits an inference that the

had been communicating with the victim via cell phone leading up to the murder gave rise to an inference that the coventurers also communicated about the crime via cell phone, particularly where the theory of the crime required a shared mental state. See Commonwealth v. Zanetti, 454 Mass. 449, 455 (2009) (joint venture theory requires that coventurers have shared mental state). Given these facts, one could infer from the affidavit that the call was related to the crime, that the crime was preplanned, and that some of that planning may have utilized cell phones, including the defendant's.

Although in isolation none of these facts would be sufficient to support a nexus between the crime and the defendant's cell phone, in determining whether an affidavit

---

T-shirt belonged to Diggs, and that he changed out of it after the shooting: a witness to the shooting stated that the shooter had a heavy build, and indicated in a showup identification that Diggs's body type matched that of the shooter. The witness stated that what Diggs was wearing during the identification was not what the shooter had worn at the time of the shooting; the shooter had been wearing a "dark top." Thus, it is likely Diggs shed the T-shirt after the shooting. Further, we infer that the size large sweatshirt belonged to either the defendant or Peters, who each had a thin build. Moreover, the attenuated connection between the parties and the defendant's girlfriend's rental car makes it unlikely that the extra clothing was there by happenstance. Thus, given our "considerable latitude . . . for the drawing of inferences," it is reasonable to infer that multiple parties changed their clothes ( citation omitted). Commonwealth v. Santiago, 452 Mass. 573, 576 (2008). See Commonwealth v. Robertson, 480 Mass. 383, 387 (2018) ("Inferences drawn from the affidavit must be reasonable and possible, but no showing that the inferences are correct or more likely true than not true is required").

supports a finding of probable cause we must take it as a whole, and not "parse[], sever[], [or] subject[] [it] to hypercritical analysis" (quotation and citation omitted). Dorelas, 473 Mass. at 501. Here, the facts add up to a nexus between the defendant's cell phone and the crime.

That equation does not, however, accord significant weight to a factor that the Commonwealth stresses. The Commonwealth argues that the defendant's use of a cell phone soon after the crime automatically implicates the phone "in an active cover up of the crime," irrespective of the additional context. See Holley, 478 Mass. at 526 (fact that codefendant was sending text messages as he was fleeing scene of crime was factor supporting nexus between crime and his cell phone). Although the defendant was using his cell phone close in time to the murder, it is unclear whether he was doing so before he saw police approaching and understood that he was about to be arrested. Even though using a cell phone while fleeing the scene of a crime may lend support to an inference that the communication is about the crime, using a cell phone just prior to or during arrest, in and of itself, does not. One might even expect that an arrestee would use a cell phone when about to be arrested. Whether it be to call one's attorney, to ask a friend or family member to post bail, or to arrange child care, using a cell phone when one is

about to be apprehended by police cannot, without more, justify a nexus to search one's cell phone.

Nothing in our decision today disturbs the holding in White, 475 Mass. 583. There, we held that to support a nexus between a crime and a cell phone, the Commonwealth needed more than evidence of a joint venture crime and the opinion of investigating officers that coventurers often use cell phones to communicate. Id. at 590. The only evidence supporting a seizure of the defendant's cell phone was that a crime had been committed by several people, that the defendant was likely one of those people, and that he owned a cell phone. Id. The detectives had no specific evidence that any cell phone had been used in the crime, or that any particular piece of evidence was likely to be found on the defendant's cell phone. Id. In short, White did not contain sufficient facts to add up to a nexus. See id.

Here, in contrast, there is more than a joint venture crime in which the participants all owned cell phones: there is evidence that the defendant made a cell phone call soon after the shooting to the person who rented the car used in the murder, there is a reasonable inference that the crime was preplanned, and there are records of threatening cell phone communications between Diggs and the victim. Thus, given these additional facts, it was reasonable to infer that the

defendant's cell phone would contain evidence related to the crime.

b. Particularity. In response to the Commonwealth's appeal, the defendant argues that the warrant was not sufficiently limited in scope.<sup>6</sup> Because the lack of particularity of the warrant may have factored into the judge's ruling, and because we are vacating the order granting the motion to suppress, we take this opportunity to provide additional guidance on the proper scope of cell phone search warrants. We hold that (1) the correct remedy for the warrant lacking particularity in this case is partial suppression; (2) the search of text messages, call logs, and Snapchat video recordings was proper;<sup>7</sup> yet (3) the lack of time restriction rendered the warrant impermissibly broad, and we must remand to determine whether the proffered evidence fell outside what would have been a reasonable temporal limit.

To determine whether a search warrant was proper in scope, we ask whether it "describe[d] with particularity the places to

---

<sup>6</sup> The defendant also argues that the eighty-day delay in seeking the warrant to search his cell phone was an additional art. 14 violation. Because this argument was not raised in the trial court, we do not consider it here. See Commonwealth v. Yasin, 483 Mass. 343, 349 (2019).

<sup>7</sup> "Snapchat is a social media website on which a member may share information with a network of 'friends.'" F.K. v. S.C., 481 Mass. 325, 327 (2019).

be searched and the items to be seized." Holley, 478 Mass. at 524, quoting Commonwealth v. Perkins, 478 Mass. 97, 106 (2017). The dual purposes of the particularity requirement are "(1) to protect individuals from general searches and (2) to provide the Commonwealth the opportunity to demonstrate, to a reviewing court, that the scope of the officers' authority to search was properly limited" (citation omitted). Holley, supra. The particularity requirement acts as "a safeguard against general exploratory rummaging by the police through a person's belongings." Commonwealth v. Freiberg, 405 Mass. 282, 298, cert. denied, 493 U.S. 940 (1989).

Although "[i]n the physical world, police need not particularize a warrant application to search a property beyond providing a specific address, . . . in the virtual world it is not enough to simply permit a search to extend anywhere the targeted electronic objects possibly could be found." Dorelas, 473 Mass. at 501-502. For a cell phone search, such a limit is akin to no limit at all. See Kerr, Digital Evidence and the New Criminal Procedure, 105 Colum. L. Rev. 279, 303 (2005) ("limiting a search to a particular computer is something like . . . limiting a search to the entire city"). "[G]iven the properties that render [a modern cell phone] distinct from the closed containers regularly seen in the physical world, a search of its many files must be done with special care and satisfy a

more narrow and demanding standard." Dorelas, 473 Mass. at 502. See Riley v. California, 573 U.S. 373, 393 (2014) (noting that searches of physical items are to cell phone searches as "a ride on horseback" is to "a flight to the moon"). We have noted that, at a minimum, the standard for the proper scope of a cell phone search must be restricted to whether the evidence "might reasonably be found in the electronic files searched." Dorelas, supra at 503 n.13.

i. Partial suppression. The Commonwealth argues that if the warrant was not properly limited in scope, the correct remedy is partial suppression only of the evidence that fell outside what would have been a reasonable scope. We agree.

The search warrant here allowed officers to search virtually every area on the cell phone, including the address book, contact list, personal calendar, date book entries, to-do lists, e-mail messages, text and video messages, photographs, video recordings, Internet browser history, and more. The officer requested permission to search "for all data described without any date restriction" because, he claimed, it was unknown "when the weapon used was acquired and when any related conspiracy may have formed." We are hard pressed to imagine what content on the cell phone might have been excluded from the broad scope that this warrant allowed. But because the Commonwealth seeks to introduce specific categories of data

only, we do not opine on the precise parameters of what would have been a reasonable search of the defendant's cell phone.

Our decision turns on whether the Commonwealth's proffered evidence would have fallen within a reasonable scope.<sup>8</sup> The defendant is not prejudiced by an overbroad warrant if the Commonwealth does not seek to exploit the lack of particularity in the warrant. Holley, 478 Mass. at 525. For example, in Commonwealth v. Hobbs, 482 Mass. 538, 550-551 (2019), we held that the defendant was not prejudiced by an overbroad warrant for three and one-half months of his cell site location information (CSLI), because the Commonwealth only introduced CSLI from the date of the crime itself. We noted that an overbroad warrant generally requires only partial suppression of the information for which there was not the requisite nexus, as long as the Commonwealth had not "relied on or otherwise

---

<sup>8</sup> Whether this determination is made on interlocutory appeal or after trial is immaterial. The concurring opinion in the Appeals Court erroneously relied on Commonwealth v. Vasquez, 482 Mass. 850, 867 (2019), for the proposition that the determination hinges on whether review is before or after trial. See Commonwealth v. Snow, 96 Mass. App. Ct. 672, 686 (2019) (Henry, J., concurring). In Vasquez, supra at 867-868, we suppressed all thirty-two days of cell site location information (CSLI) data because the Commonwealth never met its burden to establish probable cause to search the CSLI data at all, not because the warrant was overbroad. Although we commented that the search for thirty-two days of CSLI was likely overbroad, that was not the basis for suppression. Id. at 867. Full suppression was required because there was no probable cause. Id. at 868.

exploited" it at trial. Id. at 550. See Commonwealth v. Wilkerson, 486 Mass. 159, 168-169 (2020). Here, too, we believe partial suppression is the correct remedy.<sup>9</sup> Thus, we decide only whether the Commonwealth is seeking to exploit what is likely an overbroad warrant. In order to further this determination, we must analyze the specific evidence that the Commonwealth seeks to introduce from the cell phone.

ii. Content on the cell phone. After the motion to suppress had been allowed, the Commonwealth moved for permission to supplement the record with a summary of the cell phone evidence it sought to introduce. The judge agreed that such a list would provide context on appeal, and thus stated for the record what items the Commonwealth had proposed to introduce in

---

<sup>9</sup> This is not to say that partial suppression is always the correct remedy. See Wilkerson, 486 Mass. at 168 ("severance doctrine is not without limits"). In Commonwealth v. Lett, 393 Mass. 141, 145-146 (1984), we noted that "all evidence seized pursuant to a general warrant must be suppressed. The cost to society of sanctioning the use of general warrants -- abhorrence for which gave birth to the Fourth Amendment -- is intolerable by any measure" (citation omitted). See Aday v. Superior Court of Alameda County, 55 Cal. 2d 789, 797 (1961). ("We recognize the danger that warrants might be obtained which are essentially general in character but as to minor items meet the requirement of particularity, and that wholesale seizures might be made under them, in the expectation that the seizure would in any event be upheld as to the property specified. Such an abuse of the warrant procedure, of course, could not be tolerated"). The warrant here was not a general warrant, because it contained a description of the places to be searched and thus did not vest the officers with unbridled discretion. See Commonwealth v. Rutkowski, 406 Mass. 673, 675-676 (1990); United States v. Fleet Mgt. Ltd., 521 F. Supp. 2d 436, 443 (E.D. Pa. 2007).

evidence. That list included various call logs, text messages, and Snapchat video recordings.<sup>10</sup>

As discussed supra, police had probable cause to search the defendant's cell phone for evidence of the joint venture. Based on the defendant's cell phone call to his girlfriend and the inference that the coventurers could have planned some or all of the night's events beforehand, there was a substantial basis for police to search areas of the cell phone that contain communications. See, e.g., Holley, 478 Mass. at 525, 528 (search of defendants' text message communications would have been sufficiently limited in content and scope).

Communications are not limited to words. In Commonwealth v. Dorelas, 473 Mass. at 505, we noted that communications can also come in the form of photographs. There, we analyzed whether a permissible search for photographic communications included only photographs attached to text messages -- which

---

<sup>10</sup> The full list consisted of (1) text messages between the defendant and Diggs; (2) call logs between the defendant and Diggs; (3) text messages between the defendant and Peters; (4) call logs between the defendant and Peters; (5) text messages between the defendant and someone named "Sista" that referenced "Snapchatting with guns"; (6) text messages between the defendant and someone named "Staxx," which the Commonwealth interpreted as the defendant's attempt to buy a gun; and (7) three Snapchat videos -- one from November 30, 2015, that depicted the defendant with both a gun that resembled the murder weapon as well as one that did not, and two that depicted the defendant holding a gun that resembled the murder weapon. The dates of the latter two videos are unclear from the record, as are the dates of the calls and text messages.

were clearly communications -- or whether it could extend to the photograph application stored locally on the cell phone as well. Id. at 500. Because it was reasonable that communications in the form of photographs could be found there, we concluded that the search could extend to the photograph files as well. Id. at 503.

The evidence that the Commonwealth seeks to introduce here falls squarely within the realm of communications: text messages, call logs, and Snapchat video recordings. Text messages and calls are methods of communication from one party to another. Snapchat is a social media application that allows users to send or post still images or video recordings. Video recordings stored on the application have been sent, or are drafts that can be sent, from one party to another. The Snapchat video recordings are thus communications analogous to the photographs attached to text messages discussed in Dorelas, 473 Mass. at 500. Consequently, when looking for evidence related to the planning and coordination of a joint venture, it was proper here for the officers to search call logs, text messages, and Snapchat video recordings.

iii. Temporal limit. Finally, the defendant argues that the lack of any temporal limits to the search of the cell phone rendered it not sufficiently particular. We agree.

The magnitude of the privacy invasion of a cell phone search utterly lacking in temporal limits cannot be overstated. In Riley, 573 U.S. at 394, the United States Supreme Court noted that a cell phone's large storage capacity means that a search for "even just one type of information [can] convey far more than previously possible" because "the data on a phone can date back to the purchase of the phone, or even earlier." The Court noted that the "sum of an individual's private life" could be reconstructed from the contents of one's cell phone. Id.

Consequently, to be sufficiently particular, a warrant for a cell phone search presumptively must contain some temporal limit. See United States v. Winn, 79 F. Supp. 3d 904, 921 (S.D. Ill. 2015). See also United States v. Zemlyansky, 945 F. Supp. 2d 438, 459 (S.D.N.Y. 2013) (noting temporal restriction is "indic[ium] of particularity" [citation omitted]). Because of the privacy interests at stake, the temporal restriction in an initial search warrant for a cell phone should err on the side of narrowness. If, during that initial search, officers uncover information giving rise to probable cause to broaden their search of the cell phone, nothing precludes them from returning to the judge and requesting a broader warrant. As one commentator notes, this is possible because, under Riley, officers are free to seize and hold cell phones, leaving little need to carry out a search quickly. Gershowitz, The Post-Riley

Search Warrant: Search Protocols and Particularity in Cell Phone Searches, 69 Vand. L. Rev. 585, 627 (2016).

Determining the permissible parameters for a cell phone search is a "fact-intensive inquiry and must be resolved based on the particular facts of each case." Morin, 478 Mass. at 426. Similar to the nexus analysis, the inquiry can be based on "the type of crime, the nature of the [evidence] sought, and normal inferences" about how far back in time the evidence could be found (citation omitted). White, 475 Mass. at 589. For example, in a case involving the sale of stolen firearms where there is evidence that such sales usually take place quickly, the warrant should not reach back far in time. See, e.g., United States v. Roberts, 430 F. Supp. 3d 693, 717 (D. Nev. 2019) (cell phone warrant extending back four days before theft of firearms was not reasonable where sales were unlikely to have taken place until after theft). In contrast, in an insider trading case where the tenor of the parties' relationship is critical to the claim, it could be reasonable to look back further in time. See, e.g., United States v. Pinto-Thomaz, 352 F. Supp. 3d. 287, 307 (S.D.N.Y. 2018) (warrant without temporal restriction authorizing search of digital devices for information regarding relationship between parties upheld because general tenor of relationship was relevant to tipper-tippee theory and could not be confined to specific time frame).

In Holley, 478 Mass. at 525, 527-528, we noted that, although a warrant for seventeen days of text messages lacked particularity, messages exchanged two to four days before the shooting were within a reasonable temporal scope.<sup>11</sup> That determination was based on the particular facts of the case and did not amount to a general rule as to the temporal scope of cell phone searches. Such cases stand on their own facts and analysis. See id.

Here, the detective sought permission to search all of the defendant's data without any date restriction because, he claimed, "it [was] unknown as to when the weapon used was acquired and when any related conspiracy may have been formed." The affidavit did, however, contain a statement from a witness who asserted that Diggs and the victim had had a dispute "in the days leading up to the murder," as well as a statement from the defendant that he had borrowed the car earlier that day. A feud beginning mere days before, and a car borrowed earlier that day, do not support a reasonable inference that evidence related to the crime could be found in the defendant's cell phone data from years, months, or even weeks before the murder.

---

<sup>11</sup> In Holley, 478 Mass. at 510, there were two codefendants: Holley and Pritchett. We found that the Commonwealth did not exploit an insufficiently particular warrant when it introduced Holley's text messages from a period beginning two days before the shooting and Pritchett's text messages from a period beginning four days before the shooting. Id. at 525, 528.

Because the record is largely silent with respect to the dates of the Commonwealth's proposed evidence, we remand to the Superior Court for determination whether each piece of proffered evidence would have fallen within a reasonable temporal limit.<sup>12</sup>

3. Conclusion. The order allowing the defendant's motion to suppress is vacated and set aside. The matter is remanded to the Superior Court for further proceedings consistent with this opinion, including to determine whether the search exceeded the permissible scope of the warrant.

So ordered.

---

<sup>12</sup> Without knowing what search protocol was used in this case, we do not know whether any of the proffered evidence could be admissible under the plain view exception. We have noted in the past that application of the plain view doctrine to digital searches must, at least, be "limited," and we have declined squarely to decide whether the plain view doctrine applies in searches of electronic records. See Dorelas, 473 Mass. at 505 n.16; Preventive Med. Assocs. v. Commonwealth, 465 Mass. 810, 832 (2013). Here, there is no argument that any of the proffered evidence could be admissible under the plain view doctrine, and no showing that officers came across any of the data inadvertently. Thus, we do not address whether the plain view exception is applicable in this case, or in cell phone cases more generally.

Case No. 19-10842

---

**UNITED STATES COURT OF APPEALS  
FOR THE FIFTH CIRCUIT**

---

UNITED STATES OF AMERICA,

*Plaintiff-Appellee,*

v.

BRIAN MATTHEW MORTON,

*Defendant-Appellant.*

---

APPEAL FROM THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF TEXAS, FORT WORTH DIVISION  
IN CASE No. 19-CR-17-1, THE HONORABLE REED CHARLES O'CONNOR

---

**BRIEF OF *AMICI CURIAE* ELECTRONIC FRONTIER FOUNDATION,  
AMERICAN CIVIL LIBERTIES UNION, AND ELECTRONIC PRIVACY  
INFORMATION CENTER IN SUPPORT OF DEFENDANT-APPELLANT**

---

Jennifer Lynch <i>Counsel of Record</i> ELECTRONIC FRONTIER FOUNDATION 815 Eddy Street San Francisco, CA 94109 Tel: (415) 436-9333 Fax: (415) 436-9993 jlynch@eff.org	Brett Max Kaufman AMERICAN CIVIL LIBERTIES UNION FOUNDATION 125 Broad Street New York, NY 10004 Tel: (212) 549-2500	Jennifer Stisa Granick AMERICAN CIVIL LIBERTIES UNION FOUNDATION 39 Drumm Street San Francisco, CA 94111 Tel: (415) 373-0758	Alan Butler Megan Iorio Melodi Dincer ELECTRONIC PRIVACY INFORMATION CENTER 1519 New Hampshire Avenue NW Washington, DC 20036 Tel: (202) 483-1140
--	--	---	---

*Counsel for Amici Curiae*

July 13, 2021

**SUPPLEMENTAL CERTIFICATE OF INTERESTED PERSONS**

Pursuant to this Court's Rule 28.2.1, the undersigned counsel of record for *amici curiae* certify that the following additional persons and entities have an interest in the outcome of this case. These representations are made in order that the judges of this court may evaluate possible disqualification or recusal.

1. The number and style of this case are *United States v. Brian Matthew Morton*, No. 19-10842.
2. ***Amicus Curiae:*** Electronic Frontier Foundation. The Electronic Frontier Foundation is a nonprofit organization recognized as tax exempt under Internal Revenue Code § 501(c)(3). It has no parent corporation and no publicly held corporation owns 10 percent or more of its stock.
3. **Counsel for *Amicus Curiae* Electronic Frontier Foundation:** Jennifer Lynch
4. ***Amicus Curiae:*** American Civil Liberties Union. The ACLU is a nonprofit organization recognized as tax exempt under Internal Revenue Code § 501(c)(3). It has no parent corporation and no publicly held corporation owns 10 percent or more of its stock.
5. **Counsel for *Amicus Curiae* ACLU:** Jennifer Lynch, Jennifer Granick, and Brett Max Kaufman.
6. ***Amicus Curiae:*** Electronic Privacy Information Center. EPIC is a nonprofit organization recognized as tax exempt under Internal

Revenue Code § 501(c)(3). It has no parent corporation and no publicly held corporation owns 10 percent or more of its stock.

7. **Counsel for *Amicus Curiae* EPIC:** Alan Butler, Megan Iorio, and Melodi Dincer.

Dated: July 13, 2021

/s/ Jennifer Lynch  
Jennifer Lynch

**TABLE OF CONTENTS**

SUPPLEMENTAL CERTIFICATE OF INTERESTED PERSONS.....i

TABLE OF AUTHORITIES..... ii

INTEREST OF *AMICI CURIAE*..... 1

INTRODUCTION AND SUMMARY OF ARGUMENT.....3

ARGUMENT .....5

    I.    CELL PHONES CONTAIN AN IMMENSE AMOUNT OF PRIVATE,  
          SENSITIVE DATA.....5

    II.   THE FOURTH AMENDMENT REQUIRES THAT POLICE  
          DEMONSTRATE PROBABLE CAUSE TO SEARCH A CELL PHONE  
          AND THE DATA IT CONTAINS..... 10

        A.    Especially in the context of digital data searches and seizures,  
              warrants must be based on probable cause, be particularized, and  
              avoid overbreadth..... 11

        B.    Contrary to the panel opinion, facts supporting probable cause to  
              believe that a suspect is guilty of drug possession do not  
              automatically provide probable cause to search a phone. .... 13

        C.    Here, the government needed separate probable cause to search each  
              of the categories of information found on the cell phone..... 17

CONCLUSION .....27

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION,  
TYPEFACE REQUIREMENTS, AND TYPE STYLE REQUIREMENTS  
PURSUANT TO FED. R. APP. P. 32(A) .....29

CERTIFICATE OF SERVICE.....30

**TABLE OF AUTHORITIES**

**Cases**

*Arizona v. Gant*,  
556 U.S. 332 (2009).....19

*Arizona v. Hicks*,  
480 U.S. 321 (1987).....25

*Boyd v. United States*,  
116 U.S. 616 (1886).....14

*Burns v. United States*,  
235 A.3d 758 (D.C. 2020) .....20

*Commonwealth v. Snow*,  
160 N.E.3d 277 (Mass. 2021) .....23

*Commonwealth v. White*,  
59 N.E.3d 369 (Mass.2016) .....16

*Coolidge v. New Hampshire*,  
403 U.S. 443 (1971).....12

*Groh v. Ramirez*,  
540 U.S. 551 (2004).....12

*Horton v. California*,  
496 U.S. 128 (1990).....18

*Illinois v. Gates*,  
462 U.S. 213 (1983).....12, 13

*In re Search of a White Apple iPhone, Model A1332*,  
2012 WL 2945996 (S.D. Tex. 2012) .....15

*In re Search of Black iPhone 4*,  
27 F. Supp. 3d 74 (D.D.C. 2014).....22

*In re Search of Cellular Telephone Towers*,  
945 F. Supp. 2d 769 (S.D. Tex. 2013) .....15

*In re United States of America’s Application for a Search Warrant to Seize and Search Electronic Devices from Edward Cunnius*,  
770 F. Supp. 2d 1138 (W.D. Wash. 2011).....21

*Kohler v. Englade*,  
470 F.3d 1104 (5th Cir. 2006) .....12

*People v. Herrera*,  
357 P.3d 1227 (Colo. 2015).....22

*People v. Musha*,  
131 N.Y.S.3d 514 (N.Y. Sup. Ct. 2020) .....20

*People v. Thompson*,  
178 A.D.3d 457 (N.Y. App. Div. 2019) .....23

*Riley v. California*,  
573 U.S. 373 (2014)..... *passim*

*Rivera v. Murphy*,  
979 F.2d 259 (1st Cir. 1992).....13

*Stanford v. Texas*,  
379 U.S. 476 (1965).....13

*State v. Baldwin*,  
614 S.W.3d 411 (Tex. App. 2020).....14

*State v. Bock*,  
485 P.3d 931 (Or. App. 2021).....20, 24

*State v. Castagnola*,  
46 N.E.3d 638 (Ohio 2015).....16

*State v. Henderson*,  
854 N.W.2d 616 (Neb. 2014).....22

*State v. Keodara*,  
185 Wash.2d 1028 (2016).....16

*State v. Keodara*,  
364 P.3d 777 (Wash. 2015).....16

*State v. Mansor*,  
421 P.3d 323 (Or. 2018) .....16, 23, 24

*State v. Mansor*,  
81 P.3d 930 (Or. 2016) .....16

*State v. McLawhorn*,  
2020 WL 6142866 (Tenn. Crim. App. 2020) .....20

*United States v. Broussard*,  
80 F.3d 1025 (5th Cir. 1996) .....15

*United States v. Brown*,  
828 F.3d 375 (6th Cir. 2016) .....14

*United States v. Carey*,  
172 F.3d 1268 (10th Cir. 1999) .....20, 21

*United States v. Comprehensive Drug Testing, Inc.*,  
621 F.3d 1162 (9th Cir. 2010) .....24

*United States v. Galpin*,  
720 F.3d 436 (2d Cir. 2013).....18

*United States v. Garcia*,  
496 F.3d 495 (6th Cir. 2007) .....25

*United States v. Griffin*,  
555 F.2d 1323 (5th Cir. 1977) .....12

*United States v. Lyles*,  
910 F.3d 787 (4th Cir. 2018) .....15

*United States v. Morton*,  
984 F.3d 421 (5th Cir. 2021) .....14, 19

*United States v. Morton*,  
996 F.3d 754 (5th Cir. 2021) .....14

*United States v. Otero*,  
563 F.3d 1127 (10th Cir. 2009) .....12

*United States v. Walser*,  
275 F.3d 981 (10th Cir. 2001) .....21

*Warden v. Hayden*,  
387 U.S. 294 (1967).....12

*Wheeler v. State*,  
135 A.3d 282 (Del. 2016) .....16

**Other Authorities**

App Annie, *The State of Mobile 2021* (2021) .....6

App Store Preview, *Grindr* (2021).....8

App Store Preview, *Kinkoo* (2021) .....8

Apple, *Compare iPhone Models* (2021).....9

Blink, *Blink Home Monitor App* (2020).....8

Diane Thieke, *Smartphone Statistics: For Most Users, It’s ‘Round-the-Clock’ Connection*, ReportLinker (Jan. 26, 2017).....6

Geoffrey A. Fowler & Heather Kelly, *Amazon’s New Health Band Is the Most Invasive Tech We’ve Ever Tested*, Wash. Post (Dec. 10, 2020) .....7

iClick, *How Big is a Gig?* (2013).....9

Jack Nicas et al., *Millions Flock to Telegram and Signal as Fears Grow Over Big Tech*, N.Y. Times (Jan. 13, 2021) .....8

John Koetsier, *We’ve Spent 1.6 Trillion Hours on Mobile So Far in 2020*, Forbes (Aug. 17, 2020).....5

Justin McCarthy, *One in Five U.S. Adults Use Health Apps, Wearable Trackers*, Gallup (Dec. 11, 2019).....7

Logan Koepke, et al., *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones*, Upturn (Oct. 2020) .....27

Mary Meeker, *Internet Trends 2019*, Bond (June 11, 2019).....8

Mitch Strohm, *Digital Banking Survey: 76% of Americans Bank Via Mobile App— Here Are the Most and Least Valuable Features*, Forbes (Feb. 24, 2021) .....8

Nick Gallov, *55+ Jaw Dropping App Usage Statistics in 2021*, TechJury (July 4, 2021) .....7

Orin Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Tex. Tech. L. Rev. 1 (2015).....18

Pew Rsch. Ctr., *Mobile Fact Sheet* (Apr. 7, 2021).....5

Ryan Mac et al., *We Found Joe Biden’s Secret Venmo. Here’s Why That’s A Privacy Nightmare For Everyone.*, BuzzFeed News (May 14, 2021).....10

Samsung, *Galaxy S10+ 1TB (T-Mobile)* (2021) .....9

Sarah Silbert, *All the Things You Can Track with Wearables*, Lifewire (Dec. 2, 2020) .....7

Sudip Bhattacharya et al., *NOMOPHOBIA: NO MOBILE PHone PhoBIA*, 8 J. Family Med. Prim. Care (2019).....6

**INTEREST OF *AMICI CURIAE*<sup>1</sup>**

The American Civil Liberties Union (“ACLU”) is a nationwide, nonprofit, nonpartisan organization dedicated to defending the principles embodied in the Federal Constitution and our nation’s civil rights laws. The ACLU has frequently appeared before courts, including this one, throughout the country in Fourth Amendment cases, both as direct counsel and as *amicus curiae*.

The Electronic Frontier Foundation (“EFF”) is a member-supported, nonprofit civil liberties organization that works to protect free speech and privacy in the digital world. Founded in 1990, EFF has over 30,000 active donors and dues-paying members across the United States. EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law to technology. EFF regularly participates both as direct counsel and as *amicus* in the Supreme Court, this Court, and other state and federal courts in cases addressing the Fourth Amendment and its application to new technologies.

The Electronic Privacy Information Center (“EPIC”) is a public-interest research center in Washington, D.C. established to focus public attention on emerging privacy and civil liberties issues in the information age. EPIC

---

<sup>1</sup> No party’s counsel authored this brief in whole or in part. Neither any party nor any party’s counsel contributed money that was intended to fund preparing or submitting this brief. No person other than *amici*, their members, or their counsel contributed money that was intended to fund the preparing or submitting of this brief. All parties have consented to the filing of this brief.

participates as *amicus curiae* before courts across the country in cases involving constitutional rights and emerging technologies.

*Amici* have, alone or together, appeared as either counsel or *amicus* in the following cases: *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (cell-site location information); *Riley v. California*, 573 U.S. 373 (2014) (electronic device search incident to arrest); *United States v. Jones*, 565 U.S. 400 (2012) (warrantless GPS tracking); *In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600 (5th Cir. 2013) (abrogated by *Carpenter*, 138 S. Ct. 2206); *United States v. Ganius*, 824 F.3d 199 (2d Cir. 2016) (en banc) (delayed search of information seized pursuant to warrant for evidence of a different offense); *People v. Hughes*, 958 N.W.2d 98 (Mich. 2020) (similar); *Commonwealth v. Snow*, 160 N.E.3d 277 (Mass. 2021) (proper scope of warrant to search cell phone).

## **INTRODUCTION AND SUMMARY OF ARGUMENT**

Cell phones today generate and store extremely revealing information about the people who use them. The Fourth Amendment protects those people's property and privacy rights in that information, both to shield the innocent from prying government eyes and also to prevent law enforcement from rummaging through vast amounts of information that could be assembled into a story of criminal conduct, even when the government lacked probable cause to suspect any criminal conduct in the first place. Here, the panel was wrong to find that the government had probable cause to search Mr. Morton's phone, because there was no reason to believe that evidence of the crime of drug possession would be found there. The mere fact that people, including those who possess drugs, use their phones to conduct their business, is insufficient to justify expansive government searches of vast amounts of private data.

The panel was correct, however, that the scope of cell phone searches must closely adhere to the probable cause showing, lest authority to search a device for evidence of one crime mutate into authority to search the entirety of the device for evidence of any crime—a prohibited general search. Courts have many options they can deploy to ensure that investigators do not conduct general searches. Here, there was an easy path—do not grant authority to search categories of data that there is no probable cause to believe will contain evidence of the crime under

investigation. The warrant should not have included “photographs,” and the investigators should not have looked at photos because the affidavit did not support probable cause to believe that individuals in possession of drugs take pictures of themselves or otherwise preserve evidence as images.

## ARGUMENT

### **I. CELL PHONES CONTAIN AN IMMENSE AMOUNT OF PRIVATE, SENSITIVE DATA**

Smartphones are ubiquitous, highly portable devices that “place vast quantities of personal information literally in the hands of individuals.” *Riley v. California*, 573 U.S. 373, 386 (2014). Americans use their phones for a wide variety of purposes and, as a result, smartphones contain a voluminous and varied collection of data. While data is often organized by application or file type, even discrete categories of information, alone or in combination with each other, comprise a “digital record of nearly every aspect of [our] lives.” *Id.* at 375.

Cell phone use is now deeply entrenched in the fabric of daily life. Ninety-seven percent of Americans own a cell phone and 85% own a smartphone specifically.<sup>2</sup> These devices are “such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude that they were an important feature of the human anatomy.” *Riley*, 573 U.S. at 385. Mobile devices have become the screen that people access first and most often.<sup>3</sup> Nearly half of

---

<sup>2</sup> Pew Rsch. Ctr., *Mobile Fact Sheet* (Apr. 7, 2021), <https://www.pewinternet.org/fact-sheet/mobile/>.

<sup>3</sup> John Koetsier, *We’ve Spent 1.6 Trillion Hours on Mobile So Far in 2020*, *Forbes* (Aug. 17, 2020), <https://www.forbes.com/sites/johnkoetsier/2020/08/17/weve-spent-16-trillion-hours-on-mobile-so-far-in-2020/>.

Americans check their smartphones as soon as they wake up in the morning.<sup>4</sup> People proceed to spend an average of four hours a day using various apps on their phones.<sup>5</sup> Cell phone use is so persistent that the medical field has adopted a term to describe the intense anxiety many people experience when they fear being separated from their cell phones: *NOMOPHOBIA: NO MOBILE PHONE PHOBIA*.<sup>6</sup>

Americans' dependency on smartphones has, intentionally and inadvertently, resulted in our phones containing vast troves of our personal information. Indeed, cell phones "differ in both a quantitative and a qualitative sense" from other objects because of "all [the personal information] they contain and all they may reveal." *Riley*, 573 U.S. at 393, 403. The "immense storage capacity" of smartphones allows them to function as "cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers," and to store extensive historical information related to each functionality. *Id.* at 393. Because a cell phone "collects in one place many distinct types of information,"—for example, an address, a note, a prescription, a bank

---

<sup>4</sup> Diane Thieke, *Smartphone Statistics: For Most Users, It's 'Round-the-Clock' Connection*, ReportLinker (Jan. 26, 2017), <https://www.reportlinker.com/insight/smartphone-connection.html>.

<sup>5</sup> App Annie, *The State of Mobile 2021* at 7 (2021), <https://www.appannie.com/en/go/state-of-mobile-2021/>.

<sup>6</sup> Sudip Bhattacharya et al., *NOMOPHOBIA: NO MOBILE PHONE PHOBIA*, 8 J. Family Med. Prim. Care 1297 (2019), <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6510111/>.

statement, or a video—those types of information “reveal much more in combination than any isolated record,” *id.* at 394, and they reveal much more about “an individual’s private interests or concerns.” *Id.* at 395.

Cell phones collect a wide range of data about individuals through the millions of applications people download and regularly use. In 2020, the average smartphone user had forty apps installed on their phone.<sup>7</sup> Apps “offer a range of tools for managing detailed information about all aspects of a person’s life,” and the information generated by those apps “form[s] a revealing montage of the user’s life.” 573 U.S. at 396. For example, about one in five Americans currently track information related to their personal health through their mobile devices.<sup>8</sup>

Wearable devices, such as smart watches and heart rate monitors, collect additional health data, much of which is accessible via an app on the user’s cell phone.

Wearables can capture sensitive information like heart rates, location data, skin temperature, breathing rate, heat loss, and fat composition, and are sometimes used to track deeply personal events such as fertility or menstruation cycles.<sup>9</sup> Further,

---

<sup>7</sup> Nick Gallov, *55+ Jaw Dropping App Usage Statistics in 2021*, TechJury (July 4, 2021), <https://techjury.net/blog/app-usage-statistics>.

<sup>8</sup> Justin McCarthy, *One in Five U.S. Adults Use Health Apps, Wearable Trackers*, Gallup (Dec. 11, 2019), <https://news.gallup.com/poll/269096/one-five-adults-health-apps-wearable-trackers.aspx>.

<sup>9</sup> Sarah Silbert, *All the Things You Can Track with Wearables*, Lifewire (Dec. 2, 2020), <https://www.lifewire.com/what-wearables-can-track-4121040/>; Geoffrey A. Fowler & Heather Kelly, *Amazon’s New Health Band Is the Most Invasive Tech We’ve Ever Tested*, Wash. Post (Dec. 10, 2020),

apps connected to “smart” home security systems allow users to monitor and control multicamera systems from their phones, providing access to individuals’ most intimate physical spaces.<sup>10</sup> The very presence of certain dating apps can signal a person’s sexual orientation, and the data collected by such apps can reveal even more information about intimate relationships and communications.<sup>11</sup> People are also increasingly using their phones for banking and financial transactions, with roughly 76% of Americans using their primary bank’s mobile app for everyday banking tasks within the last year.<sup>12</sup> And people continue to use their phones as communication devices, with encrypted messaging platforms outpacing non-encrypted messaging services, indicating a desire for personal privacy.<sup>13</sup>

---

<https://www.washingtonpost.com/technology/2020/12/10/amazon-halo-band-review/>.

<sup>10</sup> See, e.g., Blink, *Blink Home Monitor App* (2020), <https://blinkforhome.com/blink-app>.

<sup>11</sup> See, e.g., App Store Preview, *Grindr* (2021), <https://www.grindr.com/>; App Store Preview, *Kinkoo* (2021), <https://www.kinkoo.app/>.

<sup>12</sup> Mitch Strohm, *Digital Banking Survey: 76% of Americans Bank Via Mobile App—Here Are the Most and Least Valuable Features*, *Forbes* (Feb. 24, 2021), <https://www.forbes.com/advisor/banking/digital-banking-survey-mobile-app-valuable-features/>.

<sup>13</sup> Mary Meeker, *Internet Trends 2019*, Bond at 168 (June 11, 2019), <https://www.bondcap.com/report/itr19/>; Jack Nicas et al., *Millions Flock to Telegram and Signal as Fears Grow Over Big Tech*, *N.Y. Times* (Jan. 13, 2021), <https://www.nytimes.com/2021/01/13/technology/telegram-signal-apps-big-tech.html>.

A typical smartphone today will reveal even more about a person than a *Riley*-era phone because of increased storage capacity. Storage capacities increase every year, as does the sheer volume of personal data stored on—and accessible from—cell phones. In 2014, when the Supreme Court decided *Riley*, the top-selling smartphone could store sixteen gigabytes of data. *Id.* at 394.<sup>14</sup> The minimum storage on Apple’s current line of iPhones is sixty-four gigabytes.<sup>15</sup> That is over one million Word documents, almost 40,000 photos, 32 full-length movies, and almost 15,000 songs.<sup>16</sup> Some Android models offer one terabyte of storage, roughly sixty-four times more than a *Riley*-era phone.<sup>17</sup>

A cell phone’s storage capacity allows “even just one type of information to convey far more than previously possible.” *Riley*, 573 U.S. at 394. For example, access to just the photos on a person’s phone allows “[t]he sum of [their] life [to be] reconstructed through a thousand photographs labeled with dates, locations, and descriptions.” *Id.* Access to that person’s text messages amounts to accessing

---

<sup>14</sup> Sixteen gigabytes equals about 3,680 songs, 8,672 digital copies of *War and Peace*, 9,520 digital photos, or eight feature-length movies. See iClick, *How Big is a Gig?* (2013), [https://www.iclick.com/pdf/02\\_howbigisagig\\_infographic.pdf](https://www.iclick.com/pdf/02_howbigisagig_infographic.pdf).

<sup>15</sup> Apple, *Compare iPhone Models* (2021), <https://www.apple.com/iphone/compare/>.

<sup>16</sup> iClick, *supra* note 14.

<sup>17</sup> Samsung, *Galaxy S10+ 1TB (T-Mobile)* (2021), <https://www.samsung.com/us/business/products/mobile/phones/galaxy-s/galaxy-s10-plus-1tb-t-mobile-sm-g975uckftmb/>.

“a record of all [their] communications” over long periods of time, as “the data on a phone can date back to the purchase of the phone, or even earlier” when users sync information in the cloud. *Id.* And access to a single payment app on their phone can reveal to whom they sent money, when, and for what purposes, also revealing that individual’s intimate social relationships.<sup>18</sup>

Given cell phones’ vast storage capacity, the variety of apps users have on their phones, and the detailed data contained in each of those apps, cell phones produce “a digital record of nearly every aspect of [users’] lives—from the mundane to the intimate.” *Riley*, 573 U.S. at 395. While a single app or type of data can reveal an extraordinary amount about a person, the combination of the many different types of data on a phone can essentially reconstruct a person’s life.

## **II. THE FOURTH AMENDMENT REQUIRES THAT POLICE DEMONSTRATE PROBABLE CAUSE TO SEARCH A CELL PHONE AND THE DATA IT CONTAINS**

It is axiomatic that officers must have probable cause to support the search of a cell phone. *See generally Riley*, 573 U.S. 373. Further, probable cause to search or seize *some* data on the phone cannot justify access to the totality of the phone’s contents. Given the vast amounts of personal data stored on phones and all

---

<sup>18</sup> *See* Ryan Mac et al., *We Found Joe Biden’s Secret Venmo. Here’s Why That’s A Privacy Nightmare For Everyone.*, BuzzFeed News (May 14, 2021), <https://www.buzzfeednews.com/article/ryanmac/we-found-joe-bidens-secret-venmo>.

that can be gleaned from that data, as discussed above, strict limits on searches and seizures are necessary to preserve privacy. To prevent unreasonable cell phone searches, law enforcement must specifically identify the information they have probable cause to search, and must only search that information. Otherwise, the immense amounts of personal data stored on most cell phones today will be subject to unconstitutionally overbroad searches.

In this case, officers failed to follow constitutionally required limitations. First, they failed to show probable cause in the affidavit sufficient to support a search of the phone itself. The facts of this case—an arrest for simple drug possession—do not support probable cause to search Mr. Morton’s phone at all. And second, even if there were probable cause to support a search of *some* data on the phone, the affidavit did not demonstrate that any evidence would be stored in the form of photographs.

**A. Especially in the context of digital data searches and seizures, warrants must be based on probable cause, be particularized, and avoid overbreadth.**

To safeguard our constitutional rights, courts must apply Fourth Amendment law stringently to address the unique attributes of digital data, ensuring that police direct their searches of electronic data towards evidence for which there is probable cause and away from voluminous, intimate, non-responsive private information.

The Fourth Amendment was enacted to prevent general searches, *Groh v. Ramirez*, 540 U.S. 551, 561 (2004), and to prevent the government from engaging in a “general, exploratory rummaging in a person’s belongings.” *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971). To accomplish this goal, the Fourth Amendment requires that warrants be supported by probable cause to believe that a crime was committed and that evidence of the crime will be found in the place to be searched or the thing to be seized. *Illinois v. Gates*, 462 U.S. 213, 238 (1983). Law enforcement must demonstrate “a nexus . . . between the item to be seized and [the] criminal behavior” under investigation. *United States v. Griffin*, 555 F.2d 1323, 1325 (5th Cir. 1977) (quoting *Warden v. Hayden*, 387 U.S. 294, 307 (1967)); *Kohler v. Englade*, 470 F.3d 1104, 1109 (5th Cir. 2006). Warrants must also particularly describe the things to be searched and seized. Through these fundamental limitations, properly drafted warrants prevent overbroad searches and cabin officer discretion in conducting searches or seizures.

Like personal computers, cell phones are able to “store and intermingle a huge array of one’s personal papers in a single place.” *United States v. Otero*, 563 F.3d 1127, 1132 (10th Cir. 2009). This increases the risk that law enforcement will, after seizing a digital device, be able “to conduct a wide-ranging search into a person’s private affairs, and accordingly makes the particularity requirement that much more important.” *Id.*; see also *Stanford v. Texas*, 379 U.S. 476, 511–12

(1965) (The “constitutional requirement that warrants must particularly describe the ‘things to be seized’ is to be accorded the most scrupulous exactitude when the ‘things’ are books, and the basis for their seizure is the ideas which they contain.”). To prevent every cell phone search from turning into a general search, courts must rigorously adhere to the Fourth Amendment’s probable cause requirement, both for the phone itself and for the data stored on it.

**B. Contrary to the panel opinion, facts supporting probable cause to believe that a suspect is guilty of drug possession do not automatically provide probable cause to search a phone.**

In this case, the magistrate judge issued, and the panel approved, a warrant to search Mr. Morton’s cell phone based on the officer’s training and experience that people in possession of drugs must acquire them from somewhere, and that it is likely that evidence of that transaction exists on the cell phone. (ROA.269-270) (in the officer’s experience, people use cell phones “to arrange for the illicit receipt and delivery of controlled substances”). While officers’ training and experience can often help form a basis for probable cause, there nevertheless must be some specific connection to the investigation underway, and not a general assertion that would apply to any and all such crimes. *See Gates*, 462 U.S. at 239 (“wholly conclusory statement” in affidavit is insufficient to support probable cause); *Rivera v. Murphy*, 979 F.2d 259, 263–64 (1st Cir. 1992) (officer’s “bald assertion that based on his ‘observations, training and experience,’ he had probable cause to

make the arrest” without “facts to support his legal conclusion” was insufficient); *State v. Baldwin*, 614 S.W.3d 411, 417 (Tex. App. 2020) (en banc), *petition for discretionary review granted* (Tex. 2021) (explaining why “generic, boilerplate language” about suspects’ cell phone use is insufficient to establish probable cause). Yet the panel held that, if evidence of a crime is often found in a particular location, that constitutes probable cause to believe that such evidence will be found in that location in the specific case at issue. *United States v. Morton*, 984 F.3d 421, 427 (5th Cir. 2021), *reh’g en banc granted and opinion vacated*, 996 F.3d 754 (5th Cir. 2021). Were the panel correct, law enforcement could obtain a warrant to seize and search cell phones in essentially every case. Such a result would undermine *Riley* and the Supreme Court’s recognition that cell phones, “with all they contain and all that they may reveal,” hold “the privacies of life.” *Riley*, 573 U.S. at 403 (quoting *Boyd v. United States*, 116 U.S. 616, 630 (1886)).

The panel’s conclusion is also contrary to precedent. Compare this case to that of other unlawful possession cases. Drug dealers often keep controlled substances in their homes, purses, or cars, but police are not generally permitted to search these places without investigation-specific reasons to believe evidence will be found in those places. *See, e.g., United States v. Brown*, 828 F.3d 375, 382 (6th Cir. 2016) (no probable cause to search home where affidavit contained no evidence that Brown distributed narcotics from his home, used it to store narcotics,

or that any suspicious activity had taken place there); *cf. United States v. Broussard*, 80 F.3d 1025, 1034-35 (5th Cir. 1996) (upholding search warrant where affidavit was based on officer training and experience because affidavit also contained facts linking the residence to drug trafficking); *In re Search of Cellular Telephone Towers*, 945 F. Supp. 2d 769, 770–71 (S.D. Tex. 2013) (affidavit demonstrated nexus between the records sought and the criminal activity being investigated where there was evidence that the subject used a cell phone during and in furtherance of the offense).

For similar reasons, police are not permitted to search drug suspects' cell phones in every case. *See, e.g., United States v. Lyles*, 910 F.3d 787, 794–95 (4th Cir. 2018) (affidavit that phone was inside a home where officers found “three marijuana stems in the trash” provided insufficient cause to search the phone); *In re Search of a White Apple iPhone, Model A1332*, 2012 WL 2945996, \*2 (S.D. Tex. 2012) (affidavit insufficient where government failed to establish nexus between the targeted cell phone and violation of sex-offender registration requirement, and application “seem[ed] more designed to seek evidence that the defendant may have violated statutes regarding child pornography”).

A number of state courts have rejected similar warrants where the only fact offered to support probable cause was the officer's “training and experience” that people, including criminals, use their phones and computers to communicate. As

the Massachusetts Supreme Judicial Court noted in *Commonwealth v. White*, this allegation alone is insufficient. 59 N.E.3d 369, 375 (Mass.2016). “If this were sufficient . . . it would be a rare case where probable cause to charge someone with a crime would not open the person’s cellular telephone to seizure and subsequent search.” *Id.* at 591–92 (citing *Riley*, 573 U.S. at 399 (only an “inexperienced or unimaginative law enforcement officer . . . could not come up with several reasons to suppose evidence of just about any crime could be found on a cell phone”)); *see also, e.g., State v. Castagnola*, 46 N.E.3d 638, 654 (Ohio 2015) (magistrate judge may not infer “online” activities merely because search for information was conducted by people of a certain age, nor do text messages admitting criminal activity equal probable cause to search a computer); *Wheeler v. State*, 135 A.3d 282, 288 (Del. 2016) (warrant to search a computer may not be based on boilerplate language reciting qualifications and experience of investigators without further justification why evidence of witness tampering would be found on a device); *State v. Keodara*, 364 P.3d 777, 783 (Wash. 2015), *review denied*, 185 Wash.2d 1028 (2016) (warrant affidavit alleging drug dealers keep records about their transactions on phones provided insufficient probable cause to search); *State v. Mansor*, 81 P.3d 930 (Or. 2016), *aff’d*, 421 P.3d 323 (Or. 2018) (warrant lacked probable cause where investigating officer, based on training and experience, sought information from a suspect’s computer preceding the time period relevant

to the offense).

The government's application to search Mr. Morton's phone, based only on a general assertion that people who take drugs may communicate over their phones to acquire them or discuss them, (*see* ROA.269-70), was constitutionally insufficient.<sup>19</sup> Without a specific reason to believe evidence related to the crime charged existed on the phone in *this* case, the investigators had no probable cause to have searched Mr. Morton's phone in the first place.

**C. Here, the government needed separate probable cause to search each of the categories of information found on the cell phone.**

Even if there were probable cause to search Mr. Morton's cell phone for evidence, the government could only have looked at folders and files on the device for which there was reason to believe evidence may be found. This means that, before searching texts, photographs, or emails, the government has to show that the evidence is likely to be in the form of a text, photograph, or email. Here, the government did not demonstrate a nexus between photographs and criminal behavior. Therefore, the warrant should not have included "photographs," and the investigators should not have examined them.

---

<sup>19</sup> There are many ways to procure drugs other than by text message, such as asking a friend in person, calling a drug dealer from a pay phone or landline, or loitering meaningfully on a corner.

The need for particularity and for probable cause to search each category of information found on the phone is well-grounded in Fourth Amendment jurisprudence and, contrary to the government's arguments, emphatically reinforced by the Supreme Court in *Riley*. Probable cause requires law enforcement to “know if specific information is contained on a device [before] searching it,” and it cabins searches of that data to those designed to uncover evidence of a specific crime.<sup>20</sup> If law enforcement can “search the entire electronic haystack for the needle” and “may see all the information the [entire] haystack reveals along the way,” then a warrant for all data on a phone is no different than a general warrant.<sup>21</sup> Of course, Fourth Amendment-required limitations will always be context-specific. For example, even where police are lawfully in a home, police cannot open a spice box when searching for a rifle. *See, e.g., Horton v. California*, 496 U.S. 128, 141 (1990). Nor can they rummage through a medicine cabinet while looking for a flat-screen television. *See, e.g., United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013). This basic principle is not defeated simply because potential evidence is digital rather than physical.

---

<sup>20</sup> Orin Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 *Tex. Tech. L. Rev.* 1, 3 (2015).

<sup>21</sup> *Id.*; *see also id.* at 10-11 (describing such searches as “perilously like the regime of general warrants that the Fourth Amendment was enacted to stop”).

The government argues that the panel’s holding to this effect conflicts with *Riley*. (*Pet. of the U.S. For Rehearing En Banc* at 10-11 (“U.S. *En Banc* Petition”). But *Riley* does not support the conclusion that *all* the data on a phone can be searched so long as there is a warrant for the phone. To the contrary, *Riley* explicitly discussed the invasiveness of law enforcement access to different “categories,” “areas,” “types” of data, and “apps.” *Riley*, 573 U.S. at 395, 396, 399. The Court also pointed out that electronic searches are categorically different from physical ones, and potentially result in extreme privacy intrusions. *See, e.g., id.* at 395 (“certain types of data are also qualitatively different”). Primary among the reasons the Supreme Court gave for its holding in *Riley*—that to search a cell phone seized incident to arrest, police needed to “get a warrant,” *id.* at 403—was the need to limit officer’s unbridled access to the information stored on the phone. Justifications for search, whether arrests or warrants, do not give “police officers unbridled discretion to rummage at will among a person’s private effects.” *Id.* at 399 (citing *Arizona v. Gant*, 556 U.S. 332, 345 (2009)). In other words, the lesson of *Riley* is exactly what the panel in this case said it was: “distinct types of information, often stored in different components of the phone, should be analyzed separately.” *Morton*, 984 F.3d at 425.

Indeed, with increasing frequency, courts have followed *Riley* to hold that looking in the right place, not *every* place, is the only plan that makes sense and

complies with the Constitution. *See, e.g., Burns v. United States*, 235 A.3d 758, 775 (D.C. 2020) (warrant authorizing search for categories of data for which there was no probable cause was “constitutionally intolerable”); *People v. Musha*, 131 N.Y.S.3d 514 (N.Y. Sup. Ct. 2020) (in child abuse case, there was probable cause to search the phone’s photographs, but not to examine web search history); *State v. McLawhorn*, 2020 WL 6142866, \*24–\*26 (Tenn. Crim. App. 2020) (cannot search entirety of phone to determine whether device has flashlight function); *State v. Bock*, 485 P.3d 931, 936 (Or. App. 2021) (warrant authorizing the search of a cell phone for circumstantial evidence about the owner and any evidence related to suspected criminal offenses including unlawful firearm possession was not sufficiently specific under constitution).

For example, the Tenth Circuit Court of Appeals has held that investigators may only search files for evidence related to the probable cause showing. *United States v. Carey*, 172 F.3d 1268, 1271-73 (10th Cir. 1999). In *Carey*, a police officer, pursuant to a warrant, searched a laptop for evidence of drug distribution. While searching the laptop, the officer discovered child sexual abuse material (CSAM). At this point, he began searching for and opening files he believed were likely to contain CSAM, instead of continuing to search only for evidence of drug distribution. *Id.* at 1273. The Tenth Circuit held that searching the computer data for evidence of a crime for which there was no probable cause was an

“unconstitutional general search” and violated the suspect’s expectation of privacy in data not described in the warrant. *Id.* at 1276; *see also In re United States of America’s Application for a Search Warrant to Seize and Search Electronic Devices from Edward Cunnius*, 770 F. Supp. 2d 1138, 1147–1151 (W.D. Wash. 2011) (application to search and seize “all electronically stored information . . . contained in any digital devices seized from [defendant’s] residence for evidence relating to the crimes of copyright infringement or trafficking in counterfeit goods” was improper because it sought “the broadest warrant possible,” and did not propose to use a search technique that foreclosed the plain view doctrine’s application to digital materials). By contrast, in *United States v. Walser*, which had facts similar to those in *Carey*, the investigator, upon unexpectedly finding child abuse images, “immediately ceased his search of the computer hard drive and . . . submit[ted] an affidavit for a new search warrant specifically authorizing a search for evidence of possession of child pornography.” 275 F.3d 981, 984–985 (10th Cir. 2001). Because the officer did not search images without demonstrating to a judge a nexus to the crime he was investigating, the Tenth Circuit concluded that the materials were properly admitted into evidence. *Id.* at 987. As these cases demonstrate, even when there is probable cause to search a device for *something*, data that is not connected to the probable cause showing may not be accessed or examined absent a further warrant.

And in *People v. Herrera*, the Colorado Supreme Court suppressed evidence contained in a text message involving a third party not named in the warrant. The court held that the government’s argument that *any* text message folder could be searched because of the abstract possibility that the folder might contain indicia of who owned the phone, or might have been deceptively labeled, would result in an unconstitutional limitless search. 357 P.3d 1227, ¶¶ 18, 35 (Colo. 2015). In *State v. Henderson*, the warrant permitted a search of “[a]ny and all information’ contained on the cell phone.” 854 N.W.2d 616, 633 (Neb. 2014). There, the Nebraska Supreme Court relied on *Riley* to find that the warrants were insufficiently particular because they did not refer to the specific crime being investigated. *Id.* at 633. The law is clear that police cannot get a warrant to search, nor search, information for which there is no probable cause, so a magistrate judge must reject search warrant applications asking for “all-data” on the phone without making the requisite showing. *See also, e.g., In re Search of Black iPhone 4*, 27 F. Supp. 3d 74, 79 (D.D.C. 2014).

Applying these principles, this case is straightforward. The issuing magistrate judge should have limited the warrant to specific categories of data, and the investigators should not have searched outside of those categories; photographs should have been off-limits.

Certainly, limiting searches by category of document will not always be possible. But that is no justification for discarding the Fourth Amendment’s probable cause and particularity requirements. In fact, courts have a number of options depending on the facts of the case. For example, warrants can protect against searches for evidence of past crimes as well as against broad searches justified by probable cause for minor crimes. *Riley*, 573 U.S. at 399 (warrant necessary for this purpose). Warrants can do this by specifically imposing date range limits. For example, in *State v. Mansor*, the Oregon Supreme Court held that the warrant to search the defendant’s computer should have been limited to search history on the day of a child’s injury and death, not the weeks and months before the death, as the government requested. 421 P.3d 323, 343–44 (Or. 2018) (interpreting Article I, section 9 of the Oregon Constitution). Similarly, in *Commonwealth v. Snow*, the Massachusetts Supreme Judicial Court found that a warrant to search the cell phone of a defendant accused of murder was insufficiently particular because it authorized a search without a temporal limit, even though the government argued “it was unknown ‘when the weapon used was acquired and when any related conspiracy may have been formed.’” 160 N.E.3d 277, 288 (Mass. 2021); *see also People v. Thompson*, 178 A.D.3d 457, 458 (N.Y. App. Div. 2019) (warrant to search defendant’s phones without a time limitation did not satisfy the Fourth Amendment’s particularity requirement).

Beyond category and date limitations, warrants can establish search protocols that limit the documents examined based on keywords or other search parameters, or magistrate judges can ask for search logs facilitating a post-execution review. Courts can require independent review teams to segregate relevant from irrelevant information. Courts can also impose use restrictions, as the Oregon Supreme Court did in *Mansor*, 421 P.3d at 326, or limit application of the plain view doctrine. *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1179 (9th Cir. 2010) (en banc) (Kozinski, C.J., concurring); *Bock*, 485 P.3d at 938. Depending on the circumstances of the case, there are a number of tools that can ensure that the government examines no more data than is required to accomplish a probable cause-based search.

The government's petition for rehearing *en banc* relies heavily on the argument that the panel misunderstood photographs on Mr. Morton's phone to be "places" when actually they are "things." U.S. *En Banc* Petition at p. 1, 8 ("[T]he panel's novel rule . . . confuses the "place to be searched" (the cell-phone) with the "things to be seized" (contacts, call logs, text messages, photographs)"). But it does not matter if photographs and the folders in which they are stored are "things" or "places." *Mansor*, 421 P.3d at 338 ("[T]he state's semantic observation that a computer is literally a 'thing' is a truism that does not compel a legal conclusion."). As discussed above, the Fourth Amendment requires probable cause

to seize or search papers and effects—things—just as well as places. Authorization to search a place does not equal permission to seize or examine any or all things inside that place. *See Arizona v. Hicks*, 480 U.S. 321 (1987) (officers legitimately searching a home in connection with a shooting may not also examine stereo components to access serial numbers not in plain view); *United States v. Garcia*, 496 F.3d 495 (6th Cir. 2007) (warrant to search entirety of house for cocaine did not permit search for or seizure of documents).<sup>22</sup>

In any case, a phone can be one place that nevertheless contains many other “places,” just as a home is one place that also contains other places, such as a kitchen, a bedroom, and a garage. And a place such as a home contains objects one might describe as “things” that can also be searched, like footlockers and purses. The police must have probable cause to examine each of those things, even if they are inside a place for which there is a valid warrant to search. Officers must have independent probable cause to search folders and documents stored on a phone, regardless of whether the government describes each folder or file as a “place” or a “thing.” Exactly the same, authorization to search Mr. Morton’s cell phone did not convey equal permission to examine all the places *or* things—folders, documents,

---

<sup>22</sup> Courts often analogize from physical world experience to understand digital world phenomena. These analogies are almost always inexact, and multiple analogies can be drawn, each of which could lead to a different conclusion. Here, the Court need grapple with none of these ambiguities.

or photographs—stored there.

In the government’s rehearing petition, it takes a quote from *Riley* out of context to argue for exactly the result that the Supreme Court was trying to protect against: unbridled access to digital information for which there is no probable cause. U.S. *En Banc* Pet. at p. 10 (asserting that *Riley*’s comment that “officers would not always be able to discern in advance what information would be found where on a cell phone” means that law enforcement does not need to identify in advance categories of documents, files, or folders subject to search (quoting *Riley*, 573 U.S. at 399 (quotation marks omitted))). However, that quote from *Riley* does not support the government’s argument. In context, the government in *Riley* argued that it should be allowed to access information with certain meaning—information relevant to the crime, the arrestee’s identity, or officer safety—regardless of where or how it was stored. *Id.* at 399. The Supreme Court rejected this solution as “impos[ing] few meaningful constraints on officers” in part because permission for this type of search would “sweep in a great deal of information,” especially given that officers could not know where the information would be found. *Id.* Indeed, this quote supports the *Appellant’s* position that searches must be constrained, not the government’s position to the contrary.

Despite the government’s dire warnings about the consequences of the panel’s analysis, there is nothing dangerous or radical about ensuring that

government searches of digital information comply with the longstanding principles enshrined in the Fourth Amendment that are intended to limit government authority and guarantee an active role for the judiciary. Documenting the government's reasons for searching a particular private place has been a bedrock requirement since the founding. Moreover, today's investigators have substantial tools for locating relevant information stored on a cell phone.<sup>23</sup> The practical reality is that no investigator can look at *everything* on a phone, because there is too much data. Investigators can employ technology, or even human discretion, in a manner reasonably calculated to find evidence of the crime under investigation. The Fourth Amendment dictates that warrants draw these bounds.

### **CONCLUSION**

For the reasons stated above, this court should reverse the panel's opinion finding that there was probable cause to search Mr. Morton's cell phone. In the

---

<sup>23</sup> See Logan Koepke, et al., *Mass Extraction: The Widespread Power of U.S. Law Enforcement to Search Mobile Phones*, Upturn (Oct. 2020), <https://www.upturn.org/reports/2020/mass-extraction>. Forensic tools can be far more discriminating than the government says. But even if the government described them correctly, the only reason that companies would sell such inferior tools is because the government is willing to buy them. The science required for comprehensive search is well-developed and already deployed in innumerable and publicly-available tools, such as e-discovery software, email search, image search, and the like. Forensic software companies can and will make a better tool for searching cell phones if their primary customer, the government, needs it. It would be a poor Constitution indeed that blessed the government's actions merely because the government did not pressure its forensic software providers to design better tools.

alternative, it should affirm the opinion's holding that there was no probable cause to search photographs on the device and that it unconstitutional for the government to have done so.

Dated: July 13, 2021

Respectfully submitted,

By: /s/ Jennifer Lynch  
Jennifer Lynch

ELECTRONIC FRONTIER FOUNDATION  
815 Eddy Street  
San Francisco, CA 94109  
Tel: (415) 436-9333  
Fax: (415) 436-9993  
jlynch@eff.org

Jennifer Stisa Granick  
AMERICAN CIVIL LIBERTIES UNION  
FOUNDATION  
39 Drumm Street  
San Francisco, CA 94111  
Tel: (415) 373-0758

Brett Max Kaufman  
AMERICAN CIVIL LIBERTIES UNION  
FOUNDATION  
125 Broad Street  
New York, NY 10004  
Tel: (212) 549-2500

Alan Butler  
Megan Iorio  
Melodi Dincer  
ELECTRONIC PRIVACY INFORMATION  
CENTER  
1519 New Hampshire Avenue NW  
Washington, DC 20036  
Tel: (202) 483-1140

*Counsel for Amici Curiae*

**CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME  
LIMITATION, TYPEFACE REQUIREMENTS, AND TYPE STYLE  
REQUIREMENTS PURSUANT TO FED. R. APP. P. 32(A)**

I hereby certify as follows:

1. The foregoing Brief of *Amici Curiae* complies with the type-volume limitation of Fed. R. App. P. 32(a) or Fed. R. App. P. 28.1 because this brief contains 6,279 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 365, the word processing system used to prepare the brief, in 14 point font in Times New Roman.

Dated: July 13, 2021

/s/ Jennifer Lynch  
Jennifer Lynch

**CERTIFICATE OF SERVICE**

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeal for the Fifth Circuit by using the appellate CM/ECF System on July 13, 2021. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: July 13, 2021

/s/ Jennifer Lynch  
Jennifer Lynch

United States Court of Appeals  
for the Fifth Circuit

---

No. 19-10842

---

United States Court of Appeals  
Fifth Circuit

**FILED**

January 5, 2021

Lyle W. Cayce  
Clerk

UNITED STATES OF AMERICA,

*Plaintiff—Appellee,*

*versus*

BRIAN MATTHEW MORTON,

*Defendant—Appellant.*

---

Appeal from the United States District Court  
for the Northern District of Texas  
USDC No. 4:19-CR-17-1

---

Before JOLLY, SOUTHWICK, and WILSON, *Circuit Judges.*

E. GRADY JOLLY, *Circuit Judge:*

In this appeal, we are asked to determine whether the good faith exception to the Fourth Amendment’s exclusionary rule allows officers to search the photographs on a defendant’s cellphones for evidence of drug possession, when the affidavits supporting the search warrants were based only on evidence of personal drug possession and an officer’s generalized allegations about the behavior of drug traffickers—not drug users. We hold that the officers’ affidavits do not provide probable cause to search the photographs stored on the defendant’s cellphones; and further, we hold that the good faith exception does not apply because the officers’ reliance on the

No. 19-10842

defective warrants was objectively unreasonable. And while respecting the “great deference” that the presiding judge is owed, we further hold that he did not have a substantial basis for his probable cause determination with regard to the photographs. We thus conclude that the digital images found on Morton’s cellphones are inadmissible, and his conviction is therefore VACATED. Accordingly, the case is REMANDED for further proceedings not inconsistent with this opinion.

### I.

Brian Matthew Morton was stopped for speeding near Palo Pinto, Texas. After the officers smelled marijuana, he gave consent to search his van. Officers found sixteen ecstasy pills, one small bag of marijuana, and a glass pipe. When, however, they discovered children’s school supplies, a lollipop, 14 sex toys, and 100 pairs of women’s underwear in the vehicle, they became more concerned that Morton might be a pedophile. After arresting Morton for drug possession, one of the officers, Texas Department of Public Safety (DPS) Trooper Burt Blue, applied for warrants to search Morton’s three cellphones that were found in the van. Trooper Blue’s affidavits<sup>1</sup> for the search warrants mentioned no concerns about child exploitation; instead, the warrants purported to seek more evidence of Morton’s criminal drug activity based on Trooper Blue’s training and experience—fourteen years in

---

<sup>1</sup> The affidavits and warrants were identical to each other except for naming different cellphones to be searched. The paragraph of the affidavits describing the objects of the search reads:

It is the belief of affiant that suspected party was in possession of and is concealing in [the cellphones] . . . [e]vidence of the offense of Possession of [ecstasy], possession of marijuana and other criminal activity; to wit telephone numbers, address books; call logs, contacts, recently called numbers, recently received calls; recently missed calls; text messages (both SMS messages and MMS messages); *photographs, digital images, or multimedia files in furtherance of narcotics trafficking or possession.*

No. 19-10842

law enforcement and eight years as a “DRE-Drug Recognition Expert”—as well as the drugs found in Morton’s possession and his admission that the drugs were in fact marijuana and ecstasy.

Relying on these affidavits, a judge issued warrants to search Morton’s phones. While searching the phones’ photographs, Trooper Blue and another officer came across sexually explicit images of children. The officers then sought and received another set of warrants to further search the phones for child pornography, ultimately finding 19,270 images of sexually exploited minors. The government then indicted Morton for a violation of 18 U.S.C. § 2252(a)(2) for the child pornography found on his three cellphones. The subject of drugs had vaporized.

In pretrial proceedings, Morton moved to suppress this pornographic evidence. He argued that the affidavits in support of the first set of warrants failed to establish probable cause to search for his additional criminal drug activity. The government responded by stating that the warrants were supported by probable cause and, if not, then the good faith exception to the exclusionary rule—first announced by the Supreme Court in *United States v. Leon*, 468 U.S. 897 (1984)—should apply. The district court ruled in favor of the government, and Morton later pled guilty to the child pornography charge while reserving his right to appeal the district court’s suppression decision. He was sentenced to nine years in prison, and this appeal of the suppression ruling followed.

## II.

On appeal, when examining a district court’s ruling on a motion to suppress, we review questions of law de novo and accept factual findings unless they are clearly erroneous or influenced by an incorrect view of the law. *United States v. Gentry*, 941 F.3d 767, 779 (5th Cir. 2019); *United States v. Fulton*, 928 F.3d 429, 434 (5th Cir. 2019). We view the evidence in the

No. 19-10842

light most favorable to the prevailing party. *United States v. Ganzer*, 922 F.3d 579, 583 (5th Cir. 2019). In reviewing a district court’s denial of a suppression motion for evidence obtained pursuant to a search warrant, our precedent usually applies a two-step test. *United States v. Allen*, 625 F.3d 830, 835 (5th Cir. 2010). First, we decide whether the good faith exception should apply. *Id.* If the good faith exception applies, then no further inquiry is required. *Id.* If the good faith exception does not apply, we proceed to a second step of analysis, in which we review whether the issuing judge had a substantial basis for determining that probable cause existed. *Id.*

The good faith exception to the suppression of evidence obtained in violation of the Fourth Amendment arises when an officer’s reliance on a defective search warrant is “objectively reasonable.” *United States v. Sibley*, 448 F.3d 754, 757 (5th Cir. 2006). In such a case, the evidence obtained from the search “will not be excluded.” *Id.* This court has decided that the good faith exception applies to most searches undertaken pursuant to a warrant unless one of the four situations enumerated in *Leon* removes the warrant from the exception’s protection. *Leon*, 468 U.S. at 923; see *Franks v. Delaware*, 438 U.S. 154, 171 (1978). Only one of these “exceptions to the good faith exception” is relevant here: Morton alleges that the warrant “so lack[ed] indicia of probable cause” that the officers’ reliance on it was “entirely unreasonable.” *Leon*, 468 U.S. at 923.

To determine if there were indicia of probable cause, the reviewing court will usually be required to look at the affidavit supporting the warrant, but, even so, all of the circumstances surrounding the warrant’s issuance may be considered. *United States v. Payne*, 341 F.3d 393, 400 (5th Cir. 2003); *United States v. Fisher*, 22 F.3d 574, 578 (5th Cir. 1994). Affidavits must raise a “fair probability” or a “substantial chance” that criminal evidence will be

No. 19-10842

found in the place to be searched for there to be probable cause. *Safford Unified Sch. Dist. No. 1 v. Redding*, 557 U.S. 364, 371 (2009) (cleaned up).

Here, as suggested by this court’s precedent, we turn to Trooper Blue’s affidavits supporting the search warrants. The affidavits seek approval to search Morton’s contacts, call logs, text messages, and photographs for evidence of his drug possession crimes. As the government properly conceded at oral argument,<sup>2</sup> separate probable cause is required to search each of the categories of information found on the cellphones. Although “[t]reating a cell phone as a container . . . is a bit strained,” the Supreme Court has explained that cellphones do “collect[] in one place many distinct types of information.” *Riley v. California*, 573 U.S. 373, 394, 397 (2014). And the Court’s opinion in *Riley* went to great lengths to explain the range of possible types of information contained on cellphones.<sup>3</sup>

*Riley* made clear that these distinct types of information, often stored in different components of the phone, should be analyzed separately. This requirement is imposed because “a cell phone’s capacity allows even just one

---

<sup>2</sup> Oral Argument at 27:28, *United States v. Morton*, No. 19-10842, [http://www.ca5.uscourts.gov/OralArgRecordings/19/19-10842\\_10-5-2020.mp3](http://www.ca5.uscourts.gov/OralArgRecordings/19/19-10842_10-5-2020.mp3):

The Court: Do you say you’re entitled to everything inside that phone so long as you can look at anything inside the phone?

The Government: No, your Honor.

The Court: Or do you need probable cause for each individual sort of category of information that could be found there?

The Government: That’s correct.

<sup>3</sup> *See id.* at 393 (emphasizing that the term “cellphone” is “misleading shorthand” because cellphones are in fact minicomputers that also can serve as “cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers”); *id.* at 394 (noting that “[e]ven the most basic phones” might hold photographs, messages, a calendar, a phone book, “and so on”); *id.* at 396 (describing all of the possible apps as a “range of tools for managing detailed information”).

No. 19-10842

type of information to convey far more than previously possible.” *Id.* at 394. Just by looking at one category of information—for example, “a thousand photographs labeled with dates, locations, and descriptions” or “a record of all [a defendant’s] communications . . . as would routinely be kept on a phone” — “the sum of an individual’s private life can be reconstructed.”<sup>4</sup> *Id.* at 394–95. In short, *Riley* rejected the premise that permitting a search of *all* content on a cellphone is “materially indistinguishable” from other types of searches. *Id.* at 393. Absent unusual circumstances, probable cause is required to search each category of content. *Id.* at 395 (stating that “certain types of data” on cellphones are “qualitatively different” from other types); *id.* at 400 (analyzing data from a phone’s call log feature separately); *see also Carpenter v. United States*, 138 S. Ct. 2206, 2217 (2018) (analyzing data from a phone’s cell tower location signals separately).

This distinction dovetails with the Fourth Amendment’s imperative that the “place to be searched” be “particularly describ[ed].” U.S. CONST. amend. IV.; *cf., e.g., United States v. Beaumont*, 972 F.2d 553, 560 (5th Cir. 1992) (“General warrants [which lack particularity] have long been abhorred in the jurisprudence of both England and the United States.”). Probable cause and particularity are concomitant because “—at least under some circumstances—the lack of a more specific description will make it apparent that there has not been a sufficient showing to the magistrate that the

---

<sup>4</sup> Moreover, the Supreme Court intimated in *Riley* that searching a phone may be akin to searching a defendant’s house—if not even more invasive. *Id.* at 396–97 (noting that a “cell phone search would typically expose to the government *far more than the most exhaustive search of a house*” because a phone “not only contains in digital form many sensitive records previously found in the home,” but it also “contains a broad array of private information *never found in a home in any form*”) (emphases added); *id.* at 403 (comparing general searches of cellphones to the “general warrants and writs of assistance . . . which allowed British officers *to rummage through homes* in an unrestrained search for evidence of criminal activity” against which the Founders fought) (emphasis added).

No. 19-10842

described items are to be found in a particular place.”<sup>5</sup> WAYNE R. LAFAVE, 2 SEARCH & SEIZURE § 4.5 (6th ed. 2020).

Here, this observation means that the facts as alleged in Trooper Blue’s affidavits must raise a “fair probability” or a “substantial chance” that evidence relevant to Morton’s crime—that is, simple drug possession—will be found in each place to be searched: his contacts, his call logs, his text messages, and his photographs. There must be a specific factual basis in the affidavit that connects each cellphone feature to be searched to the drug possession crimes with which Morton was initially charged.

### III.

#### A.

The affidavits successfully establish probable cause to search Morton’s contacts, call logs, and text messages for evidence of drug possession. In attesting that probable cause exists, officers may rely on their experience, training, and all the facts available to them. *Ornelas v. United States*, 517 U.S. 690, 700 (1996); *United States v. Escamilla*, 852 F.3d 474, 481

---

<sup>5</sup> This requirement is especially important in the context of searches of digital devices that contain so much content. *See, e.g.*, Adam M. Gershowitz, *The Post-Riley Search Warrant: Search Protocols and Particularity in Cell Phone Searches*, 69 VAND. L. REV. 585, 597–600 (2016); *id.* at 609 (noting that in drug cases, warrants frequently “authorize searches for photos and videos [on phones] . . . for which there is typically no probable cause”); Andrew D. Huynh, Note, *What Comes After “Get A Warrant”?: Balancing Particularity and Practicality in Mobile Device Search Warrants Post-Riley*, 101 CORNELL L. REV. 187, 190 (2015) (“The Court’s lengthy discussion about the amount of personal information accessible on a modern mobile device suggests that a search warrant’s particularity may be the next subject for scrutiny.”); William Clark, *Protecting the Privacies of Digital Life: Riley v. California, the Fourth Amendment’s Particularity Requirement, and Search Protocols for Cell Phone Search Warrants*, 56 B.C. L. REV. 1981, 1984 (2015) (“As the U.S. Supreme Court held in *Riley*, to allow the police unguided review of the entire contents of a cell phone when executing a search warrant would authorize the exact type of general warrants that the Fourth Amendment forbids.”).

No. 19-10842

(5th Cir. 2017); *Bigford v. Taylor*, 834 F.2d 1213, 1218 (5th Cir. 1988). Here, Trooper Blue relied on his fourteen years in law enforcement and eight years as a “DRE-Drug Recognition Expert” to assert that suspects’ call logs often show calls “arrang[ing] for the illicit receipt and delivery of controlled substances”; stored numbers identify “suppliers of illicit narcotics”; and text messages “may concern conversations” along these lines as well. Since this is true of drug possession suspects in general, and Morton had been found with drugs, Trooper Blue credibly alleges that there is a “fair probability” that these features of Morton’s phone would contain similar evidence of Morton’s drug possession charges.

These conclusions are supported by simple logic. To possess drugs, one must have purchased them; contacts, call records, and text messages could all easily harbor proof of this purchase. For example, text messages could show a conversation with a seller haggling over the drugs’ cost or arranging a location to meet for the exchange. Similarly, Morton could have had his source of drugs listed in his contacts as “dealer” or some similar name, and recent calls with such a person could show a recent purchase. The affidavit makes all of these points. For this reason, we hold that there was probable cause to search Morton’s contacts, call records, and text messages for evidence relating to his illegal drug possession.

## **B.**

But the affidavits also asserted probable cause to believe that the photographs on Morton’s phones contained evidence of other drug crimes, and on this claim, they fail the test of probable cause as related to the crime of possession. That is, they fall short of raising a “substantial chance” that the photographs on Morton’s phones would contain evidence pertinent to his crime of simple drug possession. As we have said, officers are permitted to rely on training and experience when attesting that probable cause exists,

No. 19-10842

but they must not turn a blind eye to details that *do not* support probable cause for the particular crime. *Bigford v. Taylor*, 834 F.2d 1213, 1218 (5th Cir. 1988) (explaining that officers may not “disregard facts tending to dissipate probable cause”).

Here, Trooper Blue supplied two facts to provide probable cause to search the images on Morton’s phones. First, Morton was found with less than two ounces of marijuana, a pipe, and sixteen pills that Morton stated were ecstasy. Second, based on Trooper Blue’s training and experience, “criminals often take photographs of co-conspirators as well as illicit drugs and currency derived from the sale of illicit drugs.” This background led Trooper Blue to assert that “*photograph images* stored in the cellular telephone may identify *other co-conspirators and show images of illicit drugs and currency derived from the sale of illicit drugs.*” These photographs would, in turn, be evidence of “other criminal activity . . . *in furtherance of narcotics trafficking*” and Morton’s drug possession crimes. The search warrant is thus expanded to seek information of an alleged narcotics trafficking conspiracy based solely on Morton’s arrest for, and evidence of, simple drug possession.<sup>6</sup>

The syllogism that Trooper Blue offers to gain access to Morton’s photographs does not provide adequate grounds for the extensive search. In

---

<sup>6</sup> In full, the sole paragraph in each affidavit purporting to provide probable cause to search Morton’s photographs reads:

Affiant knows through training and experience that photographic images taken on cellular telephones can be stored in the telephones [sic] memory and retained for future viewing. Affiant also knows through training and experience that criminals often take *photographs of co-conspirators as well as illicit drugs and currency derived from the sale of illicit drugs.* Affiant believes that photograph images stored in the cellular telephone may identify *other co-conspirators and show images of illicit drugs and currency derived from the sale of illicit drugs.*

No. 19-10842

short, the syllogism is (1) Morton was found with personal-use quantities of drugs; and (2) drug dealers often take photos of drugs, cash, and co-conspirators; it therefore follows that (3) the photographs on Morton's phones will provide evidence of Morton's relationship to drug trafficking. The fallacy of this syllogism is that it relies on a premise that cannot be established, namely that Morton was dealing drugs. And here, Trooper Blue disregarded key facts that show that the evidence did not support probable cause that Morton was a drug dealer.

To begin, the quantity of drugs Morton possessed can best be described as personal-use: a single small bag of marijuana and a few ecstasy pills. Further, Morton did not have scales, weapons, or individual plastic bags that are usually associated with those who sell drugs. It is also significant that the officers arrested Morton for possession of marijuana and ecstasy but not distribution of these drugs. *Compare* TEX. HEALTH & SAFETY CODE §§ 481.121, 481.116 *with id.* §§ 481.120, 481.113.<sup>7</sup> In sum, indications of drug trafficking were lacking: no significant amount of drugs; paraphernalia for personal use, not sale; and no large amounts of cash. Or precisely: there was *no* evidence supporting drug trafficking.

Nevertheless, Trooper Blue relied on his knowledge of the behavior of *drug traffickers* to support a search of Morton's photos. Again, we emphasize that the only times Morton's photographs are mentioned in the affidavits are in connection with statements about the behavior of drug traffickers: that "criminals often take photographs of co-conspirators as well

---

<sup>7</sup> *Cf. Moreno v. State*, 195 S.W.3d 321, 325–26 (Tex. App. 2006) (collecting cases showing that proving "delivery" under Texas law requires the consideration of factors including the quantity of contraband possessed, the presence and type of drug paraphernalia, and whether the defendant possessed a large amount of cash); *see also United States v. Le*, 512 F.3d 128, 137 (5th Cir. 2007) (Texas statutory references to "delivery" are equivalent to "possession with intent to distribute").

No. 19-10842

as illicit drugs and currency derived from the sale of illicit drugs,” and that “photograph images stored in the cellular telephone may identify other co-conspirators and show images of illicit drugs and currency derived from the sale of illicit drugs.” These suggestions relating to the behavior of *drug traffickers* may well be true,<sup>8</sup> but Trooper Blue cannot rely on these assertions to search the photo contents of the cellphones of a suspect charged with simple possession. Nor was Trooper Blue permitted, in his affidavit, to ignore the evidence that negated probable cause as to trafficking.

Since it seems that no evidence supported probable cause to believe that Morton was dealing in drugs, the affidavit leaves us with only the allegations that (1) Morton was found with drugs so (2) it therefore follows that the photographs on Morton’s phones will provide evidence of Morton’s crime of drug possession. With only this bare factual support that Morton possessed drugs, the affidavits contain nothing to link Morton’s marijuana and ecstasy with the photographs on his phones. The affidavits thus do not create a “fair probability” or a “substantial chance” that evidence of the crime of drug possession will be found in the photographs on Morton’s cellphones. Therefore, under these facts and based on the specific language in these affidavits, we hold that probable cause was lacking to search Morton’s photographs for proof of his illegal drug possession.<sup>9</sup>

---

<sup>8</sup> See, e.g., *United States v. Luna*, 797 F. App’x 158, 160 (5th Cir. 2020) (drug dealers sending photographs of guns, drugs, and cash to each other).

<sup>9</sup> This result is suggested by both our own caselaw as well as the law of other circuits. As Morton argued at oral argument (and the government could not cite a case to the contrary), our precedent is void of any cases in which personal-use quantities of drugs by themselves provide probable cause to search the photos on a defendant’s phone. Oral Argument at 41:43, *United States v. Morton*, No. 19-10842, [http://www.ca5.uscourts.gov/OralArgRecordings/19/19-10842\\_10-5-2020.mp3](http://www.ca5.uscourts.gov/OralArgRecordings/19/19-10842_10-5-2020.mp3) (“It still doesn’t get you to the images. There’s not a single case, based just on training and experience, plus cellphones, plus user-quantity drugs, that you get to get to everything in

No. 19-10842

## C.

Having demonstrated that the warrants to search the photographs stored on Morton's cellphones were not supported by probable cause, we next turn to the question of whether the evidence produced by the search may nevertheless be admitted based upon the good faith exception. To resolve this question, we ask whether the officers' good faith reliance on these defective warrants was objectively reasonable. The district court's decision on the objective reasonableness of an officer's reliance is a question of law that is reviewed de novo. *United States v. Jarman*, 847 F.3d 259, 264

---

the phone.”). And a Tenth Circuit decision similarly addresses the issues here: after arresting a defendant for drug crimes, officers applied for and received a warrant to search his computers for files containing “names, telephone numbers, ledger receipts, addresses, and other documentary evidence” of drug offenses. *United States v. Carey*, 172 F.3d 1268, 1270 (10th Cir. 1999). No drug-related evidence was found, but the officer undertaking the search also viewed the defendant's photographs and found child pornography. *Id.* at 1271. The Tenth Circuit reversed the district court, holding that these photographs should be suppressed. *Id.* at 1276.

In rejecting the government's argument that the situation was similar to “an officer having a warrant to search a file cabinet containing many drawers,” the panel held that this was “not a case in which the officers had to open each file drawer before discovering its contents.” *Id.* at 1274–75. Instead, the government “opened a drawer” marked “photographs” for which they did not have probable cause. *Id.* Subsequent Tenth Circuit cases have upheld the approach that *Carey* established, proscribing those searches with no “limiting principle” while sanctioning those that “affirmatively limit the search to evidence of . . . specific types of material” in the digital setting. *United States v. Russian*, 848 F.3d 1239, 1245 (10th Cir. 2017); *United States v. Riccardi*, 405 F.3d 852, 862 (10th Cir. 2005). Other circuits have reached similar results. *United States v. Rosa*, 626 F.3d 56, 62 (2d Cir. 2010) (concluding that a warrant to search a digital device “failed to describe with particularity the evidence sought and, more specifically, to link that evidence to the criminal activity supported by probable cause,” resulting in an impermissible “general warrant”); *United States v. Pitts*, 173 F.3d 677 (8th Cir. 1999) (noting in an analogous context outside the realm of digital searches that “when a warrant lists several locations to be searched, a court can suppress evidence recovered at a location in the warrant for which police lacked probable cause but admit evidence recovered at locations for which probable cause was established”).

No. 19-10842

(5th Cir. 2017). In reviewing whether an officer's reliance is reasonable under the good faith exception, we ask "whether a reasonably well-trained officer would have known that the search was illegal" despite the magistrate's approval. *United States v. Gant*, 759 F.2d 484, 487–88 (5th Cir. 1985).

The Supreme Court has observed: "[M]any situations which confront officers in the course of executing their duties are more or less ambiguous, [and] room must be allowed for some mistakes on their part. But the mistakes must be those of reasonable men, acting on facts leading sensibly to their conclusions of probability." *Brinegar v. United States*, 338 U.S. 160, 176 (1949). And further, "[m]ere affirmance of belief or suspicion is not enough." *Nathanson v. United States*, 290 U.S. 41, 47 (1933). The facts here lead to the sensible conclusion that Morton was a consumer of drugs; the facts do not lead to a sensible conclusion that Morton was a drug dealer. Under these facts, reasonably well-trained officers would have been aware that searching the digital images on Morton's phone—allegedly for drug trafficking-related evidence—was unsupported by probable cause, despite the magistrate's approval. Consequently, the search here does not receive the protection of the good faith exception to the exclusionary rule.

#### IV.

However, the good faith exception, applicable to the officers, does not end our analysis. As we have said, if the good faith exception does not save the search, we move to a second step: whether the magistrate who issued the warrant had a "substantial basis" for determining that probable cause to search the cellphones existed. *United States v. Allen*, 625 F.3d 830, 835 (5th Cir. 2010). While the good faith analysis focuses on what an objectively reasonable police officer would have known to be permissible, this second step focuses on the magistrate's decision. The magistrate is permitted to

No. 19-10842

draw reasonable inferences from the material he receives, and his determination of probable cause is entitled to “great deference” by the reviewing court in all “doubtful or marginal cases.” *United States v. May*, 819 F.2d 531, 535 (5th Cir. 1987); *see* 2 WAYNE R. LAFAVE ET AL., CRIMINAL PROCEDURE § 3.1(c) & n.78 (4th ed. 2019). At the same time, “a reviewing court may properly conclude that, notwithstanding the deference that magistrates deserve, the warrant was invalid because the magistrate’s probable-cause determination reflected an improper analysis.” *United States v. Leon*, 468 U.S. 897, 915 (1984).

Here, even giving the magistrate’s determination the deference due, we hold that the magistrate did not have a substantial basis for determining that probable cause existed to extend the search to the photographs on the cellphones. Even if the warrants provided probable cause to search some of the phones’ “drawers” or “file cabinets,” the photographs “file cabinet” could not be searched because the information in the officer’s affidavits supporting a search of the cellphones only related to drug trafficking, not simple possession of drugs. There was thus no substantial basis for the magistrate’s conclusion that probable cause existed to search Morton’s photographs, and the search is not saved by the magistrate’s authority. The search was unconstitutional, not subject to any exceptions, and the evidence must be suppressed as inadmissible.

## V.

Today, we have held that a reasonably well-trained officer would have known that probable cause was lacking to search the photographs stored on the defendant’s cellphones for evidence related to drug possession, which was the only crime supporting a search. Moreover, we have held that any additional assertions in the affidavits were too minimal and generalized to provide probable cause for the magistrate to authorize the search of the

No. 19-10842

photographs. Because the officers' search of the stored photographs pursuant to the first warrants was impermissible, obviously the use of that information—which was the evidence asserted to secure the second set of warrants—tainted the evidence obtained as a result of that second search, making it the unconstitutional “fruit of the poisonous tree.” *See, e.g., United States v. Martinez*, 486 F.3d 855, 864 (5th Cir. 2007). Therefore, the evidence obtained as a result of the second set of warrants is inadmissible.

As we have earlier noted, Morton pled guilty while reserving the right to appeal the district court's order on the motion to suppress. This conditional guilty plea, under Federal Rule of Criminal Procedure 11(a)(2), allows a defendant to “reserv[e] in writing the right to have an appellate court review an adverse determination of a specific pretrial motion.” FED. R. CRIM. P. 11(a)(2). Furthermore, “a defendant who prevails on appeal may then withdraw [his] plea.” *Id.* Therefore, as to the photographs discovered in the first search of Morton's cellphones and the subsequently discovered evidence from the second searches, we REVERSE the order of the district court denying Morton's motion to suppress, VACATE Morton's conviction and sentence so that he may withdraw his plea, and REMAND this case to the district court for further proceedings not inconsistent with this opinion.

REVERSED, VACATED, and REMANDED.

No. 18-30121

---

**IN THE UNITED STATES COURT OF APPEALS  
FOR THE NINTH CIRCUIT**

---

UNITED STATES OF AMERICA,

*Plaintiff-Appellee,*

v.

KALEB BASEY

*Defendant-Appellant.*

On Appeal from the United States District Court  
for the District of Alaska, Fairbanks  
No. 4:14-cr-00028-RRB-1  
Hon. Ralph R. Beistline

---

**BRIEF OF AMICI CURIAE AMERICAN CIVIL LIBERTIES UNION &  
AMERICAN CIVIL LIBERTIES UNION OF ALASKA FOUNDATION  
IN SUPPORT OF DEFENDANT-APPELLANT KALEB BASEY**

---

Brett Max Kaufman  
Patrick Toomey  
American Civil Liberties Union  
Foundation  
125 Broad Street  
New York, NY 10004  
(212) 549-2500

Jennifer Stisa Granick  
American Civil Liberties Union  
Foundation  
39 Drumm Street  
San Francisco, CA 94111  
(415) 621-2493

*Counsel for Amici Curiae*

## **CORPORATE DISCLOSURE STATEMENT**

Amici Curiae American Civil Liberties Union (“ACLU”) and ACLU of Alaska Foundation are non-profit entities that do not have parent corporations. No publicly held corporation owns 10 percent or more of any stake or stock in amici curiae.

Date: February 19, 2019

/s/ Jennifer Stisa Granick  
Jennifer Stisa Granick

*Counsel for Amici Curiae*

## TABLE OF CONTENTS

TABLE OF AUTHORITIES .....	iii
STATEMENT OF INTEREST.....	1
INTRODUCTION .....	2
STATUTORY AND FACTUAL BACKGROUND .....	3
ARGUMENT .....	9
I. The Government’s Use of Section 2703(f) in Mr. Basey’s Case Violated the Fourth Amendment.....	9
A. The Government Compelled Yahoo! to Copy and Preserve Mr. Basey’s Private Data for Nine Months Without a Warrant.....	10
B. The Fourth Amendment Protects the Content of Email Communications Against Warrantless Searches and Seizures. ....	12
C. Yahoo! Acted as a Government Agent When It Copied and Preserved Mr. Basey’s Email Account Pursuant to Section 2703(f).....	18
D. The Copying and Preservation of Mr. Basey’s Emails Was a Seizure Under the Fourth Amendment. ....	20
E. The Government’s Warrantless Seizure of Mr. Basey’s Private Information Was Unreasonable.....	21
F. Section 2703(f) Forces Providers to Perform Unconstitutional Seizures on Behalf of Law Enforcement.....	26
CONCLUSION.....	28

## TABLE OF AUTHORITIES

### Cases

<i>Ajemian v. Yahoo!, Inc.</i> , 478 Mass. 169 (2017) .....	18
<i>Berger v. New York</i> , 388 U.S. 41 (1967).....	15
<i>Camara v. Municipal Ct.</i> , 387 U.S. 523 (1967).....	22
<i>City of Ontario v. Quon</i> , 560 U.S. 746 (2010).....	13
<i>Ex parte Jackson</i> , 96 U.S. 727 (1877).....	13
<i>Eysoldt v. ProScanImaging</i> , 194 Ohio App. 3d 630 (2011).....	18
<i>Groh v. Ramirez</i> , 540 U.S. 551 (2004).....	22
<i>Hoffa v. United States</i> , 385 U.S. 293 (1966).....	15
<i>Horton v. California</i> , 496 U.S. 128 (1990).....	20
<i>In re Grand Jury Subpoena</i> , 828 F.3d 1083 (9th Cir. 2016) .....	13
<i>In the Matter of the Search of premises known as: Three Hotmail Email accounts</i> , No. 16-MJ-8036-DJW, 2016 WL 1239916 (D. Kan., Mar. 28, 2016).....	8, 9
<i>In the Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation</i> , 829 F.3d 197 (2d Cir. 2016) .....	19
<i>Johnson v. United States</i> , 333 U.S. 10 (1948).....	22

<i>Katz v. United States</i> , 389 U.S. 347 (1967).....	12, 13, 15
<i>Kentucky v. King</i> , 563 U.S. 452 (2011).....	24
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001).....	13
<i>Loretto v. Teleprompter Manhattan CA TV Corp.</i> , 458 U.S. 419 (1982).....	15
<i>Mincey v. Arizona</i> , 437 U.S. 385 (1978).....	25, 26, 27
<i>Minnesota v. Dickerson</i> , 508 U.S. 366 (1993).....	22
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014).....	12
<i>Ryburn v. Huff</i> , 565 U.S. 469 (2012).....	24
<i>San Jose Charter of the Hells Angels Motorcycle Club v. City of San Jose</i> , 402 F.3d 962 (9th Cir. 2005) .....	23
<i>Sandoval v. Cty. of Sonoma</i> , 912 F.3d 509 (9th Cir. 2018) .....	22
<i>Soldal v. Cook Cty.</i> , 506 U.S. 56 (1992).....	14, 21
<i>United States v. 1982 Sanger 24' Spectra Boat</i> , 738 F.2d 1043 (9th Cir. 1984) .....	15
<i>United States v. Biasucci</i> , 786 F.2d 504 (2d Cir. 1986) .....	16
<i>United States v. Camou</i> , 773 F.3d 932 (9th Cir. 2014) .....	24, 25, 27

<i>United States v. Carpenter</i> , 138 S. Ct. 2206 (2018).....	14, 23
<i>United States v. Carpenter</i> , 484 U.S. 19 (1987).....	15
<i>United States v. Chadwick</i> , 433 U.S. 1 (1977).....	22
<i>United States v. Forrester</i> , 512 F.3d 500 (9th Cir. 2008) .....	13
<i>United States v. Freitas</i> , 800 F.2d 1451 (9th Cir.1986) .....	15
<i>United States v. General Motors Corp.</i> , 323 U.S. 373 (1945).....	15
<i>United States v. Hawkins</i> , 249 F.3d 867 (9th Cir. 2001) .....	22
<i>United States v. Heckenkamp</i> , 482 F.3d 1142 (9th Cir. 2007) .....	16, 23
<i>United States v. Huguez-Ibarra</i> , 954 F.2d 546 (9th Cir. 1992) .....	23
<i>United States v. Jacobsen</i> , 466 U.S. 109 (1984).....	13, 20
<i>United States v. McCormick</i> , 502 F.2d 281 (9th Cir. 1974) .....	22
<i>United States v. Microsoft</i> , 138 S. Ct. 1186 (2018).....	20
<i>United States v. Miller</i> , 688 F.2d 652 (9th Cir. 1982) .....	19
<i>United States v. Ojeda</i> , 276 F.3d 486 (9th Cir. 2002) .....	24

<i>United States v. Place</i> , 462 U.S. 696 (1983).....	21, 26
<i>United States v. Reed</i> , 15 F.3d 928 (9th Cir. 1994) .....	19
<i>United States v. Taborda</i> , 635 F.2d 131 (2d Cir. 1980) .....	16
<i>United States v. Torres</i> , 751 F.2d 875 (7th Cir. 1984) .....	16
<i>United States v. Warshak</i> , 631 F.3d 266 (6th Cir. 2010) .....	12, 13, 16, 23
<i>Warden v. Hayden</i> , 387 U.S. 294 (1967).....	24

**Statutes**

18 U.S.C. § 2703 .....	passim
755 Ill. Comp. Stat. 70/1 .....	18
Alaska Stat. Ann. § 13.63.040 .....	17
Ariz. Rev. Stat. Ann. § 14-13101.....	18
Cal. Penal Code § 1546.1.....	17
Cal. Prob. Code §§ 870–84.....	18
Colo. Rev. Stat. Ann. § 15-1-1501.....	18
Conn. Gen. Stat. Ann. § 45a .....	18
Del. Code Ann. tit. 12, § 5001 .....	18
Fla. Stat. § 740.001 .....	18
Hawaii Rev. Stat. § 556a-1 .....	18
Idaho Code § 15-14-101 .....	18
Ind. Code § 32-39-1-1.....	18

Md. Code Ann. Est. & Trusts § 15-601 .....	18
Mich. Comp. Laws § 700.1001.....	18
Minn. Stat. § 521a.01 .....	18
Mo. Const. art. I, § 15 .....	16
N.C. Gen. Stat. Ann. § 3f-1.....	18
N.Y. Est. Powers & Trusts Law § 13-a-1 .....	18
Neb. Rev. Stat. § 30-501 .....	18
S.C. Code Ann. § 62-2-1010.....	18
Tenn. Code Ann. § 35-8-101 .....	18
Tex. Prop. Code Ann. § 111.004 .....	16
U.S. Const. amend. IV .....	12
Wash. Rev. Code Ann. § 11.120.010.....	18
Wisc. Stat. § 711.01 .....	18
Wisc. Stat. Ann. § 711 .....	18

**Other Authorities**

<i>Access to Digital Assets of Decedents,</i> Nat’l Conf. of state Legs. (Dec. 3, 2018).....	17
Becca Stanek, <i>Missouri Passes Constitutional Amendment to Protect Electronic Privacy</i> , Time Magazine, Aug. 6, 2014 .....	17
Black’s Law Dictionary (10th ed. 2014) .....	14
DOJ, <i>Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations</i> (2015).....	5, 6
Facebook, <i>Transparency Report: Government Requests (United States)</i> .....	7, 8
FBI, <i>Domestic Investigations and Operations Guide 18-126</i> (2016) .....	5

Google, *Transparency Report: Requests for User Information (United States)* .....7

Natalie M. Banta, *Inherit The Cloud: The Role of Private Contracts in Distributing or Deleting Digital Assets At Death*,  
83 Fordham L. Rev. 799 (2014).....17

Orin Kerr, *The Fourth Amendment and Email Preservation Letters*,  
Wash. Post: The Volokh Conspiracy, Oct. 28, 2016.....9

## STATEMENT OF INTEREST<sup>1</sup>

The American Civil Liberties Union (“ACLU”) is a nationwide, nonprofit, nonpartisan organization with more than two million members and supporters dedicated to the principles of liberty and equality embodied in the Constitution and our nation’s civil rights laws. Since its founding in 1920, the ACLU has frequently appeared before the Supreme Court and other federal courts in numerous cases implicating Americans’ right to privacy, including as counsel in *Carpenter v. United States*, 138 S. Ct. 2206 (2018), and as amicus in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010).

The ACLU of Alaska Foundation is an Alaska non-profit corporation dedicated to advancing civil liberties in Alaska; it is an affiliate of the American Civil Liberties Union. Like the national organization, the ACLU of Alaska Foundation has a long-time interest in protecting Alaskan’s rights to privacy. The members and supporters of the ACLU of Alaska Foundation include individuals statewide who seek to ensure that they and their family members and friends receive fair and just treatment in the courts.<sup>2</sup>

---

<sup>1</sup> All parties consent to the filing of this brief. No party or party’s counsel authored this brief or contributed money to fund the preparation or submission of this brief. No person other than amici, their members, and their counsel contributed money to fund the preparation or submission of this brief.

<sup>2</sup> Amici would like to thank Melodi Dincer and Kristin M. Mulvey, students in the Technology Law & Policy Clinic at NYU School of Law, for their contributions to this brief.

## INTRODUCTION

Investigators in this case relied on 18 U.S.C. § 2703(f) to compel Yahoo! to copy and preserve Mr. Basey's emails and other account data—without getting a warrant—for nine months. This prolonged, warrantless seizure is typical of a growing nationwide practice: one where investigators regularly issue secret demands to preserve individuals' private account data just in case they decide to return with a court order later. Based on public transparency reports, federal and state investigators rely on section 2703(f) to copy and preserve private electronic data tens or hundreds of thousands of times each year. None of these demands require any showing of suspicion, need, or exigency.

The copying and preservation of Mr. Basey's emails and account data violated the Fourth Amendment. When Yahoo! secretly duplicated Mr. Basey's private data at the government's direction, it was acting as a government agent—and thus this seizure of his information was subject to Fourth Amendment constraints. In the absence of a warrant, copying and preserving these messages was an unconstitutional seizure of private information. A warrantless seizure can be justified by exigent circumstances if the government has good cause to preserve the data for a short while to seek a warrant. But if any exigency existed in this case—and none is apparent from the record—it dissipated over the nine months that the government delayed before applying for a warrant. Moreover, section

2703(f) is problematic because in most cases investigators appear to be using it to unconstitutionally seize private communications. The statute does not require probable cause, a risk that evidence will be destroyed, or that investigators promptly submit a court application to obtain the data they have preserved. While there may well be cases where the short-term, warrantless copying and preservation of private data is reasonable, this case is not one of them. The Court should hold that the government's protracted, warrantless seizure of Mr. Basey's private data violated the Fourth Amendment.

### **STATUTORY AND FACTUAL BACKGROUND**

Every year, investigators use section 2703(f) to warrantlessly copy and preserve—for months at a time—the private data in tens or hundreds of thousands of internet accounts, including Mr. Basey's. This takes place because section 2703(f) gives law enforcement the power to unilaterally, and without suspicion or judicial approval, compel electronic communications service providers like Yahoo! to copy and preserve their users' email accounts.

The Stored Communications Act (“SCA”) regulates government access to user data stored by electronic communications service providers (hereinafter “providers”), including Yahoo!. Under the SCA, some types of information, including certain account-related metadata, can be compelled from providers with a subpoena, while more sensitive data, including emails and other electronic

communications, require a court order or a search warrant. 18 U.S.C. § 2703. By contrast, section 2703(f) of the SCA establishes a procedure whereby investigators may themselves, without any judicial involvement, compel providers to make a copy of email messages and other account data, and preserve that copy for 90 days “pending the issuance of” legal process (or 180 days, with a renewal). The provider must comply.

Section 2703(f) reads:

(1) In general.—

A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention.—

Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90-day period upon a renewed request by the governmental entity.

Both the statutory text and the DOJ’s own internal guidance documents indicate that the purpose of section 2703(f) is to give investigators the ability to ensure that relevant evidence will not be destroyed before law enforcement can obtain the requisite legal process compelling disclosure of private data.<sup>3</sup> The statute itself indicates that the government demand must be a precursor to seeking

---

<sup>3</sup> It is not clear that section 2703(f) permits law enforcement to seize the *content* of communications at all. The statute refers to “records and other evidence” and a “court order or other process.” It does not specifically reference communications content nor the search warrants required to seize and search that information.

judicial authorization to obtain and search the data: requests must be made “pending the issuance of a court order or other process.” 18 U.S.C. § 2703(f)(1). The Department of Justice (“DOJ”) manual for Searching and Seizing Computers describes section 2703(f) as a means of preserving evidence so that it will not be “destroyed or lost before law enforcement can obtain the appropriate legal order compelling disclosure.” DOJ, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 139 (2015), available at <https://perma.cc/XYF8-J2KG>. And the FBI’s Domestic Investigations and Operations Guide instructs investigators that in order “to make a preservation request, the FBI must believe that the records will subsequently be sought by appropriate legal process.” FBI, *Domestic Investigations and Operations Guide* 18-126 (2016), available at <https://perma.cc/4DDY-942B>.

However, the statute does not require Fourth Amendment safeguards. It does not require probable cause at the time law enforcement issues a copy and preservation demand. It does not require that there be a risk that evidence will be destroyed. Nor does it obligate investigators to seek legal process in a reasonable amount of time under the facts and circumstances of the case. Instead, it permits seizing information for up to 180 days without judicial oversight.

In practice, investigators issue tens or hundreds of thousands of boilerplate preservation demands under section 2703(f) each year—and often never return

with additional legal process. DOJ advises investigators to seek preservation “as soon as possible” after an investigation commences, and it provides a template for investigators to fill out. *See* DOJ, App. C Sample Language for Preservation Requests under 18 U.S.C. § 2703(f), *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 225–26 (2015), available at <https://perma.cc/XYF8-J2KG>. When investigators do return with a court order authorizing a search of the targeted account, they commonly wait months to do so. In theory, section 2703(f) appears intended to preserve records in cases where investigators have concrete intentions to seek legal process. But in practice, investigators regularly use the statute to force providers to copy and preserve tens or hundreds of thousands of private online accounts *just in case* a need for the information arises later in the course of an investigation.

Unsurprisingly, because section 2703(f) does not require probable cause or individualized suspicion and an independent judicial check—and because the government can issue demands under the statute quickly and simply—the volume of preservation demands is extremely high. Since at least July 2014, Google has annually received tens of thousands of 2703(f) letters requesting preservation of multiple user accounts—including 8,698 letters affecting 22,030 accounts in the

first half of 2018 alone.<sup>4</sup> Google, *Transparency Report: Requests for User Information (United States)*, <https://perma.cc/MP98-8SCP> (last visited Feb. 19, 2019). In that same six-month period, Facebook received 57,000 preservation letters for 96,000 different accounts. Facebook, *Transparency Report: Government Requests (United States)*, <https://perma.cc/TVV5-QYW9> (last visited Feb. 19, 2019) (“Facebook Transparency Report”). In recent years, these numbers have been rising. Comparing to the six-month period between July and December 2017 with the period between January and June 2018, Google and Facebook together experienced between 20% and 30% increases in section 2703(f) letters and affected accounts.

In some of these instances, investigators eventually meet the constitutional and statutory standards required to search private account data by subsequently serving appropriate legal process on providers. But providers receive thousands more section 2703(f) letters than they do subsequent legal process to actually search the accounts. For example, in the most recent six-month reporting period, Facebook received a total of 57,000 section 2703(f) letters, but only received 23,801 search warrants, 9,369 subpoenas, and 942 section 2703(d) court orders.

---

<sup>4</sup> One letter can require a provider to copy and retain emails and other data from more than one account.

*Id.*<sup>5</sup> Even assuming—implausibly—that legal process is always tied to an account previously targeted by a section 2703(f) letter, investigators never demonstrated any basis for their demands to copy and preserve accounts on almost 23,000 occasions over six months. From this data, it appears that the government’s actual use of section 2703(f) is not primarily about preservation of evidence in cases where investigators are actively seeking a warrant. Rather, section 2703(f) provides investigators with a powerful tool to routinely copy and preserve tens of thousands of accounts without any evidence, risk of spoliation, judicial oversight, or obligation to follow-up.

Making matters worse, investigators appear to rarely formally renew section 2703(f) demands (or seek related judicial process) within the statutorily provided 90-day retention period—or even within 180 days, after the one renewal contemplated by the statute. Indeed, one district court recently noted that the case at issue was “the first time the Court can remember the government indicating it renewed its preservation request” within the allotted 90 days. *In the Matter of the Search of premises known as: Three Hotmail Email accounts*, No. 16-MJ-8036-DJW, 2016 WL 1239916, at \* 12 n.78 (D. Kan., Mar. 28, 2016), *overruled in part on other grounds*, 212 F. Supp. 3d 1023 (D. Kan. 2016). According to the court, it

---

<sup>5</sup> Section 2703(d) allows the government to obtain certain account data upon a showing of “specific and articulable facts showing that there are reasonable grounds to believe that [the data sought] are relevant and material to an ongoing criminal investigation.”

was also “the first time the Court can remember the government *seeking* a search warrant within that one-time renewal period, as seems to be the intent of subsection (f).” *Id.* There, the records were preserved beyond the 180-day statutory maximum and it appears the government never requested an extension of time.<sup>6</sup>

As both data and anecdote demonstrate, law enforcement officers regularly send section 2703(f) requests as a “matter of course,” copying and preserving troves of personal data for months at a time, without any showing of cause or need. Orin Kerr, *The Fourth Amendment and Email Preservation Letters*, Wash. Post: The Volokh Conspiracy, Oct. 28, 2016, <https://wapo.st/2IdmLjv> (“[T]he preservation authority is routinely used by the government to preserve contents of communications. . . . And it turns out that a lot of investigators and prosecutors issue such letters often.”). As explained above, this offends the statute—and, as discussed below—the Fourth Amendment as well.

## ARGUMENT

### **I. The Government’s Use of Section 2703(f) in Mr. Basey’s Case Violated the Fourth Amendment.**

The government’s use of section 2703(f) to copy and preserve Mr. Basey’s email account data violated the Fourth Amendment. Although warrantless seizures of email accounts may be justified in certain cases involving exigent circumstances, this case is not one of them. Congress could write a statute that

---

<sup>6</sup> As discussed below, the same sequence of events occurred in this case.

lawfully requires providers to temporarily retain data at risk of spoliation for a short period of time while law enforcement seeks a warrant. But section 2703(f) authorizes law enforcement to seize emails—private property—far beyond what the Fourth Amendment allows. Without probable cause, or case-specific reasons to believe that evidence will be destroyed, the statute forces communications providers to copy and preserve communications for months at a time. These seizures are unconstitutional.

**A. The Government Compelled Yahoo! to Copy and Preserve Mr. Basey’s Private Data for Nine Months Without a Warrant.**

The government’s use of section 2703(f) in this case exemplifies how investigators regularly rely on this provision to carry out protracted, warrantless seizures of personal communications.

In this case, three law enforcement agencies were investigating Mr. Basey for attempted enticement of a minor in violation of 18 U.S.C. § 2422(b), receipt of child pornography in violation of 18 U.S.C. § 2252(a)(2) and (b)(1), and distribution of child pornography in violation of 18 U.S.C. § 2252(a)(2) and (b)(1). Indictment, *United States v. Basey*, No. 4:14-cr-00028-RRB (D. Alaska Dec. 16, 2014). These agencies included the Alaska State Troopers (“AST”), the United States Army Criminal Investigation Command (“CID”), and the Federal Bureau of Investigation (“FBI”). Br. for Appellant at 2–3, *United States v. Basey*, No. 18-3012 (9th Cir. Feb. 12, 2019), ECF No. 26. As part of the investigation, in January

of 2014, officials seized Basey's electronic devices. *Id.* at 6. Almost one month later, on February 7, 2014, CID agent Shanahan sent a section 2703(f) letter to Yahoo!, requiring the company to preserve Basey's email account for 90 days. *Id.* at 6. Four days later, on February 11, Yahoo! confirmed with investigators that it had preserved Basey's account. *Id.* at 6–7. From May to June of 2014, AST searched Basey's devices (but not his Yahoo! account) pursuant to a military search warrant. *Id.* Based on information obtained through this search, AST and CID then contacted the FBI, which used a subpoena to obtain Craigslist<sup>7</sup> postings sent from Basey's Yahoo! email address. *Id.* Finally, on November 11, 2014—more than nine months after issuing a section 2703(f) demand to Yahoo!—the FBI secured a warrant for the Yahoo! account. The FBI then obtained the data preserved under section 2703(f) and searched Basey's Yahoo! emails, producing the evidence used to convict him in this case.

This use of section 2703(f) is typical in that investigators do not appear to have issued the demand when they were actively seeking a warrant to take possession of and search Mr. Basey's Yahoo! data—nor did they obtain legal process within the statutorily prescribed time period. These failures both afflicted this investigation, and also fit a pattern that appears common in criminal

---

<sup>7</sup> Craigslist is a popular online forum hosting classified advertisements for jobs, housing, items wanted and for sale, as well as discussion forums.

investigations that involve potential searches of digital data—which, in today’s world, is practically all investigations.

**B. The Fourth Amendment Protects the Content of Email Communications Against Warrantless Searches and Seizures.**

The Fourth Amendment provides that:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

U.S. Const. amend. IV. The Fourth Amendment protects both an individual’s reasonable expectation of privacy and her property rights. This constitutional protection means that the government generally must obtain a warrant before searching or seizing private property. *Katz v. United States*, 389 U.S. 347, 357 (1967).

Email and other electronic communications are among those personal effects protected by the Fourth Amendment. Email can contain the most private and personal messages imaginable. *See, e.g., Riley v. California*, 134 S. Ct. 2473, 2490, 2494–95 (2014). Today we use email and text messages to “send sensitive and intimate information, instantaneously, to friends, family, and colleagues half a world away. Lovers exchange sweet nothings, and businessmen swap ambitious plans, all with the click of a mouse button.” *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010). Email and other electronic communications have become

so pervasive that many would “consider them to be essential means or necessary instruments for self-expression, even self-identification.” *City of Ontario v. Quon*, 560 U.S. 746, 760 (2010); *see Warshak*, 631 F.3d at 284 (“Since the advent of email, the telephone call and the letter have waned in importance, and an explosion of Internet-based communications has taken place.”); *see also Kyllo v. United States*, 533 U.S. 27, 28 (2001) (cautioning that advances in technology must not “erode the privacy guaranteed by the Fourth Amendment”).

Because of its sensitivity, the Fourth Amendment protects email and other similar modes of communication from unreasonable searches and seizures. *See Katz*, 389 U.S. at 353; *United States v. Jacobsen*, 466 U.S. 109, 114 (1984) (“Letters and other sealed packages are in the general class of effects in which the public at large has a legitimate expectation of privacy[.]”); *In re Grand Jury Subpoena*, 828 F.3d 1083, 1090 (9th Cir. 2016) (“Personal email can, and often does, contain all the information once found in the ‘papers and effects’ mentioned explicitly in the Fourth Amendment.”); *United States v. Forrester*, 512 F.3d 500, 511 (9th Cir. 2008) (holding that “[t]he privacy interests in [mail and email] are identical”); *Warshak*, 631 F.3d at 284, 288 (holding that an individual enjoys a reasonable expectation of privacy in the contents of emails); *cf. Ex parte Jackson*, 96 U.S. 727, 733 (1877) (Fourth Amendment protects letters in transit). Indeed, in the Supreme Court’s recent opinion in *United States v. Carpenter*, every Justice

agreed, at least in dicta, that the Fourth Amendment protects the content of emails. *See* 138 S. Ct. 2206, 2222 (2018) (majority op.); *id.* at 2230 (Kennedy, J., dissenting, joined by Thomas and Alito, JJ.); *id.* at 2262, 2269 (Gorsuch, J., dissenting).<sup>8</sup>

Widespread adoption of email and other electronic communications has led to a societal recognition that these materials are extremely private. That recognition goes hand in hand with the longstanding possessory interest people have in their email messages, as well as the growing number of statutes that seek to manage property rights in intangible data.

Like the privacy interest, the Fourth Amendment also protects the property interest in email. The Fourth Amendment protects an individual's possessory interest in her papers and effects. *See Soldal v. Cook Cty.*, 506 U.S. 56, 62–64, 68 (1992) (explaining that a seizure occurs when one's property rights are violated, even if the property is never searched). Possessory interest is defined as the present “right to control property, *including the right to exclude others*, [even] by a person who is not necessarily the owner.” Black's Law Dictionary (10th ed. 2014) (emphasis added); *United States v. 1982 Sanger 24' Spectra Boat*, 738 F.2d 1043,

---

<sup>8</sup> Besides communications content, an email subscriber may have a reasonable expectation of privacy in other categories of account information, such as certain account metadata. Since the government seized the content of Basey's communications, this Court need not decide here whether the Fourth Amendment also protects the other types of data that the government seized when it directed Yahoo! to preserve Basey's account.

1046 (9th Cir. 1984); *Loretto v. Teleprompter Manhattan CA TV Corp.*, 458 U.S. 419, 435 (1982) (“The power to exclude has traditionally been considered one of the most treasured strands in an owner’s bundle of property rights.”). A possessory interest also includes the right to delete or destroy the property. *United States v. General Motors Corp.*, 323 U.S. 373, 378 (1945) (Property rights in a physical thing have been described as the rights “to possess, use and dispose of it.” (quotation marks omitted)); *cf. United States v. Carpenter*, 484 U.S. 19, 26 (1987) (“Confidential business information has long been recognized as property.”).

Email has these canonical characteristics of property. Users have the right to exclude others from their accounts. Users protect their accounts with passwords. Providers encrypt user emails both in transit and when stored on servers in order to exclude outsiders. Email users also have the right to delete their email messages. Providers allow users to delete single messages, or the entire account. And even though email is intangible, it is still property subject to Fourth Amendment protections. *Hoffa v. United States*, 385 U.S. 293, 301 (1966) (Fourth Amendment protections are “surely not limited to tangibles . . . .”); *United States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir.1986) (“[S]urreptitious searches and seizures of intangibles strike at the very heart of the interests protected by the Fourth Amendment.”); *Katz*, 389 U.S. at 353; *Berger v. New York*, 388 U.S. 41, 54–60 (1967) (telephone conversations); *United States v. Biasucci*, 786 F.2d 504, 509–10

(2d Cir. 1986) (video surveillance); *United States v. Torres*, 751 F.2d 875, 883 (7th Cir. 1984) (video surveillance); *United States v. Tabora*, 635 F.2d 131, 139 (2d Cir. 1980) (enhanced visual surveillance inside the home). Moreover, the Fourth Amendment protects emails even if a provider’s terms of service or privacy policy allow government access under certain circumstances, as almost all do. Courts have considered and rejected arguments to the contrary. *See, e.g., Warshak*, 631 F.3d at 286 (“While . . . a subscriber agreement might, in some cases, be sweeping enough to defeat a reasonable expectation of privacy in the contents of an email account . . . we doubt that will be the case in most situations . . . .”); *United States v. Heckenkamp*, 482 F.3d 1142, 1146-47 (9th Cir. 2007) (policies establishing limited instances of access do not vitiate Fourth Amendment interests).

State laws recognize that individuals are the owners of the data in their email accounts. State legislatures are increasingly recognizing a property right in electronic communications. For example, the Texas Property Code defines “[p]roperty” for the purposes of trust management as “including property held in any digital or electronic medium.” Tex. Prop. Code Ann. § 111.004(12) (2017). Missouri amended its state constitution in 2014 to protect “persons, papers, homes, effects, *and electronic communications and data*, from unreasonable searches and seizures[.]” Mo. Const. art. I, § 15 (emphasis added); *see also* Becca Stanek, *Missouri Passes Constitutional Amendment to Protect Electronic Privacy*, Time

Magazine, Aug. 6, 2014, <https://perma.cc/56D3-RUUR>. Similarly, California’s Electronic Communications Privacy Act prohibits government entities from compelling production of or access to electronic communications without a warrant. Cal. Penal Code § 1546.1 (2016).

In some states, legislatures have made clear that email account information is property in the context of determining rights after incapacity or death. Over the past several years, a wave of state legislatures enacted laws addressing access to “digital assets,” including email accounts, upon a person’s incapacity or death. *See generally Access to Digital Assets of Decedents*, Nat’l Conf. of State Legs. (Dec. 3, 2018), <https://perma.cc/Z35T-AS45>; Natalie M. Banta, *Inherit The Cloud: The Role of Private Contracts in Distributing or Deleting Digital Assets At Death*, 83 *Fordham L. Rev.* 799, 801 (2014) (defining “digital assets” to “include an individual’s email accounts”). These laws extend fiduciary duties to electronic communications as another form of property that can be held in trust. For example, Alaska’s Fiduciary Access to Digital Assets Act conditions disclosure of the electronic communications of a deceased user upon their prior consent or on a court order. Alaska Stat. Ann. § 13.63.040 (2017). Since 2013, at least 46 states have enacted similar laws regulating fiduciary duties with respect to digital assets, all of which explicitly recognize a deceased or incapacitated user’s legal interest in

access to their email communications.<sup>9</sup> Wisconsin’s version is of particular note, as the statutory chapter is entitled “Digital Property.” Wisc. Stat. Ann. § 711 (2016).

Additionally, some state courts have also begun to expand common law property principles to better protect digital communications. *See, e.g., Ajemian v. Yahoo!, Inc.*, 478 Mass. 169, 170 (2017) (finding e-mail accounts are a “form of property often referred to as a ‘digital asset’”); *Eysoldt v. ProScanImaging*, 194 Ohio App. 3d 630, 638 (2011) (permitting conversion action of web account as intangible property).

Because email is private personal property, it is protected by the Fourth Amendment from unreasonable searches and seizures.

**C. Yahoo! Acted as a Government Agent When It Copied and Preserved Mr. Basey’s Email Account Pursuant to Section 2703(f).**

Although the Fourth Amendment does not apply to private entities, Yahoo! acted as a government agent here when it copied and preserved Basey’s email at

---

<sup>9</sup> *See, e.g.,* Ariz. Rev. Stat. Ann. §§ 14-13101 to -13118 (2016); Cal. Prob. Code §§ 870–84 (2017); Colo. Rev. Stat. Ann. §§ 15-1-1501 to -1518 (2016); Conn. Gen. Stat. Ann. §§ 45a-334b-339 (2016); Del. Code Ann. tit. 12, §§ 5001-5007 (2015); Fla. Stat. §§ 740.001-.09 (2016); Hawaii Rev. Stat. §§ 556a-1 to -17 (2016); Idaho Code §§ 15-14-101 to -119 (2016); 755 Ill. Comp. Stat. 70/1 to -21 (2016); Ind. Code §§ 32-39-1-1 to -2-15 (2016); Md. Code Ann. Est. & Trusts §§ 15-601 to -620 (2016); Mich. Comp. Laws §§ 700.1001-.1018 (2016); Minn. Stat. §§ 521a.01-.19 (2016); Neb. Rev. Stat. §§ 30-501 to 508 (2016); N.Y. Est. Powers & Trusts Law §§ 13-a-1 to -5.2 (2016); N.C. Gen. Stat. Ann. §§ 3f-1 to -18 (2016); S.C. Code Ann. §§ 62-2-1010 to -1090 (2016); Tenn. Code Ann. §§ 35-8-101 to 118 (2016); Wash. Rev. Code Ann. §§ 11.120.010-.901 (2016); Wisc. Stat. § 711.01 (2016).

the government's behest. Yahoo!'s actions, then, must comply with the Fourth Amendment.

Private entities are state actors when the government directs their activities. In *United States v. Miller*, this Court created a two-prong test to discern whether a private individual is acting as a governmental agent or instrument for Fourth Amendment Purposes: “(1) whether the government knew of and acquiesced in the intrusive conduct, and (2) whether the party performing the search intended to assist law enforcement efforts or to further [their] own ends.” 688 F.2d 652, 657 (9th Cir. 1982); see *United States v. Reed*, 15 F.3d 928, 931 (9th Cir. 1994).

When companies comply with section 2703(f) letters, they are acting as agents of the government—just as they are when they actually retrieve and produce customer data in response to court-approved legal process. Here, Yahoo!, a private company, acted as a governmental agent because (1) the investigating agencies involved in Mr. Basey's case not only knew of but directed the search and seizure, and (2) Yahoo! preserved Mr. Basey's entire email account for the purpose of complying with investigators' section 2703(f) demand, not for its own purposes. See *In the Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, 829 F.3d 197, 214 (2d Cir. 2016) (holding, in another case involving the Stored Communications Act, that “[w]hen the government compels a private party to assist it in conducting a search or seizure,

the private party becomes an agent of the government” under the Fourth Amendment), *vacated as moot by United States v. Microsoft*, 138 S. Ct. 1186 (2018).

**D. The Copying and Preservation of Mr. Basey’s Emails Was a Seizure Under the Fourth Amendment.**

When the government sent Yahoo! a section 2703(f) demand requiring copying and preservation of Basey’s email and other messages, it was a Fourth Amendment seizure. A Fourth Amendment “seizure” of property occurs when “there is some meaningful interference with an individual’s possessory interests in that property.” *Jacobsen*, 466 U.S. at 113; *Horton v. California*, 496 U.S. 128, 133 (1990). Yahoo!’s compliance meant that Basey could no longer exclude the government from accessing, searching, using, or sharing his private messages and associated data. It meant that he could no longer delete his messages. Because of the receipt of the 2703(f) letter, whatever the user did to his information, a copy would nevertheless remain for government use. That copying and preservation meaningfully interfered with his possessory interests—and thus constituted a Fourth Amendment seizure.

The government may argue that it neither took possession of nor reviewed Basey’s emails prior to obtaining a warrant. This is irrelevant. The warrantless seizure took place at the point in time when the government’s agent, Yahoo!, copied the account data. Human examination is not required for a seizure. Rather, a

seizure occurs when police secure or detain private property so that they may search it later. The Supreme Court has flatly rejected the view that the Fourth Amendment only protects property seizures where there is a corresponding privacy or liberty invasion. *See Soldal*, 506 U.S. at 62–65 (holding that dragging away a mobile home was a seizure even though officers had not entered the house, rummaged through the possessions, or detained the owner). Similarly, in *United States v. Place*, the seized a container and did not allow anyone to touch it or its contents while the police obtained a search warrant—but the Court held this was a seizure governed by the Fourth Amendment. 462 U.S. 696, 707 (1983) (“There is no doubt that the agents made a ‘seizure’ of Place’s luggage for purposes of the Fourth Amendment when, following his refusal to consent to a search, the agent told Place that he was going to take the luggage to a federal judge to secure issuance of a warrant.”). Likewise, private account data is seized at the moment that providers copy and preserve that information pursuant to the government’s demand. The section 2703(f) letter process interferes with an email account holder’s Fourth Amendment-protected interests even if an investigator never examines the materials.

**E. The Government’s Warrantless Seizure of Mr. Basey’s Private Information Was Unreasonable.**

The government seized Basey’s emails without a warrant when Yahoo! copied the data for investigators. The record here does not justify this warrantless

seizure, especially not for nine months. The seizure of Basey’s emails was unreasonable and unconstitutional.

It is a cardinal Fourth Amendment rule that “[a] seizure conducted without a warrant is per se unreasonable . . . subject only to a few specifically established and well-delineated exceptions.” *Sandoval v. Cty. of Sonoma*, 912 F.3d 509, 515 (9th Cir. 2018); *United States v. Hawkins*, 249 F.3d 867, 872 (9th Cir. 2001) (quoting *Minnesota v. Dickerson*, 508 U.S. 366, 372 (1993)). “When the right of privacy must reasonably yield to the right of search (and seizure) is, as a rule, to be decided by a judicial officer, not by a policeman or Government enforcement agent.” *United States v. McCormick*, 502 F.2d 281, 285 (9th Cir. 1974) (quoting *Johnson v. United States*, 333 U.S. 10, 14 (1948)). Review by a neutral and objective judicial magistrate who weighs the importance of the constitutional safeguards of the Fourth Amendment with law enforcement interests helps ensure law enforcement actions are not abusive or unjustified. The purpose of requiring a warrant is to minimize the risk of “arbitrary invasions by governmental officials” to the “privacy and security of individuals[.]” *Camara v. Municipal Ct.*, 387 U.S. 523, 528 (1967). The warrant process ““assures the individual whose property is searched or seized of the lawful authority of the executing officer, his need to search, and the limits of his power to search.”” *Groh v. Ramirez*, 540 U.S. 551, 561 (2004) (quoting *United States v. Chadwick*, 433 U.S. 1, 9 (1977)). In other words,

the warrant specifically describing the items to be seized legitimates an officer's authority to seize those items. *See San Jose Charter of the Hells Angels Motorcycle Club v. City of San Jose*, 402 F.3d 962, 973 (9th Cir. 2005).

Here, no warrant authorized the government's seizure of Mr. Basey's email account. Thus, the government bears the burden of showing that its warrantless seizure falls "under one of a few specifically established exceptions to the warrant requirement." *United States v. Huguez-Ibarra*, 954 F.2d 546, 551 (9th Cir. 1992). No exception applies.

The government may argue that Basey consented to the seizure of his account via the Yahoo! terms of service or privacy policy. But these materials do not vitiate users' Fourth Amendment interests. Courts have repeatedly rejected the argument that they do. *See e.g., Warshak*, 631 F.3d at 286; *Heckenkamp*, 482 F.3d at 1146-47; *Carpenter*, 138 S. Ct. at 2220; *see also supra* Section I.B. Nearly every terms of service and privacy policy states that the provider may disclose information pursuant to valid legal process and legal requests. That is a statement of fact, not an expression of consent. If these notices authorized warrantless seizures and searches, most of our email communications would lack Fourth Amendment protection. As the courts have repeatedly made clear, that is hardly the case.

More to the point, the government may argue that this warrantless seizure was justified to preserve evidence pending investigators' application for a search warrant. Under the exigency exception to the warrant requirement, a warrantless search or seizure may nevertheless be constitutional if: "(1) [officers] have probable cause to believe that the item or place . . . contains evidence of a crime, and (2) they are facing exigent circumstances that require immediate police action." *United States v. Camou*, 773 F.3d 932, 940 (9th Cir. 2014); *see United States v. Ojeda*, 276 F.3d 486, 488 (9th Cir. 2002). The circumstances must "cause a reasonable person to believe that entry or search was necessary to prevent physical harm . . . the destruction of relevant evidence, the escape of the suspect, or some other consequence improperly frustrating legitimate law enforcement efforts." *Camou*, 773 F.3d at 940 (alterations and citations omitted). Thus, the exigency exception applies when officers are in "hot pursuit" of a fleeing suspect, the suspect might threaten the safety of police or others, or when evidence of the crime or contraband might be destroyed. *See Warden v. Hayden*, 387 U.S. 294 (1967) (fleeing suspect); *Ryburn v. Huff*, 565 U.S. 469 (2012) (threat of injury); *Kentucky v. King*, 563 U.S. 452, 455 (2011) (destruction of contraband).

The government has not met its burden to establish exigency here. The record does not appear to establish probable cause to seize or search Basey's email account at the time investigators sent the section 2703(f) letter to Yahoo!. Email

accounts contain highly sensitive information and the invasion of privacy and interference with property is extreme. Without probable cause, the government has no demonstrable right to the information, and its seizure is unreasonable. *See Camou*, 773 F.3d at 940.

The need to preserve evidence that might be destroyed can justify a warrantless seizure, but only for as long as the exigency lasts. The exigency exception is limited to the length of the exigency itself. *See Mincey v. Arizona*, 437 U.S. 385 (1978). A warrantless search or seizure under the exigency exception must be limited in scope so that it is “strictly circumscribed by the exigencies which justify its initiation.” *Id.* at 393. At some point, the duration of a seizure can exceed the time required to promptly prepare and obtain a warrant—rendering the seizure unreasonable.

If investigators reasonably believed that the contents of Mr. Basey’s account could be destroyed, it is beyond imagination that exigency lasted for nine months—beyond even what the statute permits. Even if initially copying Basey’s emails was lawful, retaining them for nine months was not. The Fourth Amendment governs both the initial copying of data and also its retention. Given how strong the individual’s privacy and property interests are, and the weak government interest in stockpiling private communications in the absence of any genuine exigency, this ongoing retention was unreasonable as well. In *Mincey*, the

Supreme Court held that a four-day long warrantless search of appellant's apartment following a shoot-out was impermissible, even though the investigators were initially legitimately at the premises and investigating a murder. *Mincey*, 437 U.S. at 394. In *Place*, the Court suppressed evidence obtained after investigators detained the defendant's luggage for ninety minutes. *Place*, 462 U.S. at 696, 710. The Court held that "the length of the detention of respondent's luggage *alone* precludes the conclusion that the seizure was reasonable in the absence of probable cause." *Id.* at 709 (emphasis added).

Thus, in both *Mincey* and *Place*, an initial seizure was justified by exigency. But prolonged interferences with Fourth Amendment interests converted lawful police action into unconstitutional ones. Likewise, here, because the government compelled the retention of Basey's data long past any time period necessary to obtain legal process, that seizure was unreasonable.

**F. Section 2703(f) Forces Providers to Perform Unconstitutional Seizures on Behalf of Law Enforcement.**

The statute authorizes warrantless seizures that last 90 days by default and are untethered from any showing of exigency. The Fourth Amendment requires more than that to justify such a warrantless intrusion. Section 2703(f) states that a provider must preserve records "pending the issuance of a court order or other process." But the statute does not contain any judicial oversight, notice, or obligation to seek a warrant within a reasonable amount of time. 18 U.S.C.

§ 2703(f). As a result, investigators routinely copy and preserve private email account information just in case. Sometimes the police come back for the data months later. Sometimes they do not. *See supra* Statutory and Factual Background. Meanwhile, the most sensitive of our personal materials is preserved in anticipation of government perusal at some undetermined future point.

The need to preserve evidence is a legitimate law enforcement interest. But officers must have probable cause to believe that the item contains evidence of a crime, and must be facing exigent circumstances that require immediate police action. *Camou*, 773 F.3d 932, 940. Section 2703(f) also does not limit the seizures it authorizes to the *length* of the exigency as the Fourth Amendment requires. *Mincey*, 437 U.S. 385. Instead, section 2703(f) provides a 90- or 180-day retention period, regardless of the facts of the case. It is hard to imagine any situation where the government has the requisite probable cause but needs 90 days or more to seek a warrant.

Congress could pass a statute that would lawfully obligate providers to preserve account information in exigent circumstances. At the very least, a constitutional statute would authorize law enforcement to make preservation demands if investigators have probable cause, are in the process of seeking a warrant, and there is a risk of spoliation. In that situation, upon receipt of the demand, a provider could be required copy and retain the data for a short period of

time while the government applies for the warrant. Unfortunately, to the detriment of tens or even hundreds of thousands of people each year, this is not what section 2703(f) does.

## CONCLUSION

Mr. Basey's emails were warrantlessly seized for nine months, an unreasonable amount of time for law enforcement to interfere with an individual's powerful constitutional interest in these private and personal digital papers. For these reasons, this Court should hold that the government's seizure of Mr. Basey's Yahoo! emails pursuant to section 2703(f) violated the Fourth Amendment.

Date: February 19, 2019

Respectfully submitted,

/s/ Jennifer Stisa Granick  
American Civil Liberties Union  
Foundation  
Jennifer Stisa Granick  
39 Drumm Street  
San Francisco, CA 94111-4805

Brett Max Kaufman  
Patrick Toomey  
American Civil Liberties Union  
Foundation  
125 Broad Street  
New York, NY 10004  
(212) 549-2500

*Counsel for Amici Curiae*

## CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify that:

This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,553 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionately spaced typeface using Times New Roman 14-point font.

Date: February 19, 2019

/s/ Jennifer Stisa Granick  
Jennifer Stisa Granick

## **CERTIFICATE OF SERVICE**

I hereby certify that on February 19, 2019, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system.

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

Date: February 19, 2019

*/s/ Jennifer Stisa Granick*  
Jennifer Stisa Granick

NOT FOR PUBLICATION

FILED

UNITED STATES COURT OF APPEALS

AUG 14 2019

FOR THE NINTH CIRCUIT

MOLLY C. DWYER, CLERK  
U.S. COURT OF APPEALS

UNITED STATES OF AMERICA,

No. 18-30121

Plaintiff-Appellee,

D.C. No. 4:14-cr-00028-RRB

v.

MEMORANDUM\*

KALEB L. BASEY,

Defendant-Appellant.

Appeal from the United States District Court  
for the District of Alaska  
Ralph R. Beistline, District Judge, Presiding

Argued and Submitted August 5, 2019  
Anchorage, Alaska

Before: TALLMAN, IKUTA, and N.R. SMITH, Circuit Judges.

Kaleb Basey was convicted by a jury of one count of transportation of child pornography and one count of distribution of child pornography, in violation of 18 U.S.C. § 2252(a)(1), (a)(2), and (b)(1). Basey appeals the district court's denials of his request for a continuance in order to file additional suppression motions, his motion to dismiss the indictment on speedy trial grounds, and his motion for

---

\* This disposition is not appropriate for publication and is not precedent except as provided by Ninth Circuit Rule 36-3.

judgment of acquittal under Federal Rule of Criminal Procedure 29. We have jurisdiction under 28 U.S.C. § 1291, and we affirm.

1. We review the denial of a motion to continue for abuse of discretion. *See United States v. Soto*, 794 F.3d 635, 655 (9th Cir. 2015). It is undisputed that Basey made his request for a continuance to file additional suppression motions: (a) twelve days before trial was set to begin; (b) eight months after the last stated pretrial motions deadline; and (c) following two complete rounds of pretrial suppression motions he had previously filed. Basey’s renewed request was untimely under Federal Rule of Criminal Procedure 12(c)(3), and he was required to show good cause why the district court nevertheless should consider it. *See United States v. Tekle*, 329 F.3d 1108, 1112 (9th Cir. 2003) (addressing then-current Rule 12(f)). Based on this record, we cannot say that the district court abused its discretion when it denied Basey’s motion to continue.<sup>1</sup>

2. We review the district court’s denial of a Sixth Amendment speedy trial

---

<sup>1</sup> We reject Basey’s argument that the district court must have reached the merits of his proposed motions in denying the continuance because it stated that the motions “all appear to be without merit on their face.” Because the court made no findings (explicit or implicit) respecting whether Basey’s email account was seized under 18 U.S.C. § 2703(f) in violation of the Fourth Amendment, let alone whether his emails should be suppressed, *cf. United States v. Scott*, 705 F.3d 410, 416 (9th Cir. 2012) (to constitute a ruling on the merits of a waived or forfeited suppression argument, a court’s order must actually determine whether seized evidence should have been suppressed), we are not persuaded that the merits, and not the untimely nature of the motion, was the basis of the court’s ruling.

claim de novo, reviewing the underlying findings of fact for clear error. *See United States v. Sutcliffe*, 505 F.3d 944, 956 (9th Cir. 2007). To determine whether Basey’s Sixth Amendment rights were violated, we must balance “the length of the delay, the reason for the delay, the defendant’s assertion of his right, and prejudice to the defendant.” *United States v. Tanh Huu Lam*, 251 F.3d 852, 855 (9th Cir. 2001) (citing *Barker v. Wingo*, 407 U.S. 514, 529 (1972)). Though the delay in this case was long enough to trigger the *Barker* balancing test, we conclude that the balance of factors here ultimately does not weigh in Basey’s favor.

The second *Barker* factor—the reason for the delay—is the “focal inquiry” in the analysis. *See United States v. King*, 483 F.3d 969, 976 (9th Cir. 2007). The district court’s finding that Basey was largely responsible for the delay is not clearly erroneous. The record supports the court’s conclusion that most, if not all, of the delay was due to the sequential manner in which Basey chose to file his pretrial motions and his decision to change counsel less than a month before his trial date. As to the third factor, Basey did not assert his right to a speedy trial until after all of his other pretrial motions had been resolved and he was approaching the eve of trial. This does not “strongly counsel in favor of finding a Sixth Amendment violation.” *Id.* Finally, while Basey’s pretrial confinement—whether measured from the date of the superseding indictment or the first indictment—was

lengthy, it still must be “balanced and assessed in light of the other *Barker* factors, including the . . . reasons[] and responsibility for the delay.” *Lam*, 251 F.3d at 860. Under the circumstances of this case, we conclude that Basey’s Sixth Amendment right to a speedy trial was not violated since he was primarily responsible for delays.

3. We review de novo the denial of a Rule 29 motion for acquittal and examine the sufficiency of the evidence to convict. *See United States v. Tisor*, 96 F.3d 370, 379 (9th Cir. 1996). Here, the evidence at trial, taken in the light most favorable to the prosecution, was sufficient for a rational juror to find the essential elements of Basey’s crimes beyond a reasonable doubt and the venue properly laid in the District of Alaska.<sup>2</sup> *See United States v. Doe*, 842 F.3d 1117, 1119 (9th Cir. 2016). Even assuming that the child pornography distribution charge at issue here required proof that a recipient opened the email attachment of a pornographic image, the jury reasonably could have concluded from the emails produced at trial that the recipient of Basey’s email did so. Likewise, as to his claim that venue was not proper in Alaska, a rational fact finder could conclude that it was more likely than not that Basey emailed a child pornography image to himself on October 22, 2013, while he was in Fairbanks, Alaska, and that venue there was proper.

---

<sup>2</sup> Venue need only be shown by a preponderance of the evidence. *See United States v. Lukashov*, 694 F.3d 1107, 1120 (9th Cir. 2012).

**AFFIRMED.**