NO. 15-CF-322

Argued April 18, 2017

IN THE DISTRICT OF COLUMBIA COURT OF APPEALS

PRINCE JONES,
Defendant-Appellant,
v.
UNITED STATES OF AMERICA,
***Plaintiff-Appellee*.**

On Appeal from the Superior Court of the District of Columbia Criminal Division, No. 2013-CF1-18140

SUPPLEMENTAL BRIEF OF THE AMERICAN CIVIL LIBERTIES UNION, AMERICAN CIVIL LIBERTIES UNION OF THE DISTRICT OF COLUMBIA,† AND ELECTRONIC FRONTIER FOUNDATION AS AMICI CURIAE

† The American Civil Liberties Union of the District of Columbia was previously known as the American Civil Liberties Union of the Nation's Capital.

NATHAN FREED WESSLER *
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
T: (212) 549-2500
F: (212) 549-2654
nwessler@aclu.org

JENNIFER LYNCH
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
T: (415) 436-9333
jlynch@eff.org

ARTHUR B. SPITZER
SCOTT MICHELMAN
AMERICAN CIVIL LIBERTIES UNION OF THE DISTRICT OF COLUMBIA
4301 Connecticut Avenue, N.W., Suite 434
Washington, D.C. 20008
T: (202) 457-0800
F: (202) 457-0805
aspitzer@acludc.org

Table of Contents

Table of Authorities

Cases

Question Presented

In its order of April 20, 2017, this Court *sua sponte* sought supplemental briefing addressing the following question:

> What reasonable and legitimate expectation of privacy does a person have in his or her location information when the person possesses (outside his or her residence) a stolen cell phone capable of being located by a cell-site simulator or through real-time cell-site location information available to the cell phone owner or his or her telecommunications provider?

Amici Curiae American Civil Liberties Union, American Civil Liberties Union of the District of Columbia, and Electronic Frontier Foundation address this question herein.

Argument

I. The mere fact of a suspect's apparent possession of stolen cell phones does not permit law enforcement to track the suspect's own cell phone without a warrant.

A. Under the Fourth Amendment, a person's reasonable expectation of privacy is a function of both the information the government acquires *and* the means the government uses to acquire it.

Under the Fourth Amendment, where a government search impinges on a person's reasonable expectation of privacy, the search is "per se unreasonable" unless conducted pursuant to a judicial warrant. *City of L.A. v. Patel*, 135 S. Ct. 2443, 2452 (2015) (quoting *Arizona v. Gant*, 556 U.S. 332, 338 (2009)). As explained in amici's initial brief, the Metropolitan Police Department's ("MPD") use of a cell site simulator to surreptitiously track and precisely locate Defendant's cell phone violated his reasonable expectation of privacy and required a valid warrant. Corrected Br. of the American Civil Liberties Union et al. as Amici Curiae, at 2–10; *see also State v. Andrews*, 134 A.3d 324, 327 (Md. Ct. Spec. App. 2016) ("We conclude that people have a reasonable expectation that their cell phones will not be used as real-time tracking devices by law enforcement, and—recognizing that the Fourth Amendment protects people and not simply areas—that people have an objectively reasonable expectation of privacy in real-time cell phone location information. Thus, we hold that the use of a cell site simulator requires a valid search warrant . . . .").

That Defendant was in possession of stolen cell phones does not diminish his reasonable expectation that the government would not "surreptitious[ly] conver[t] . . . [*his*] cell phone into a tracking device and [engage in] the electronic interception of location data from *that* cell phone." *Andrews*, 134 A.3d at 348 (emphasis added). For Fourth Amendment purposes, it matters not only *what* information the government obtains, but also *how* it obtains it and from *where*. In other words, "[w]hether a defendant had a legitimate expectation of privacy in certain information depends in part on what the government did to get it." *United States v. Carpenter*, 819 F.3d 880, 888 (6th Cir. 2016), *petition for cert. filed* (No. 16-402); *accord United States v. Dzwonczyk*, No. 4:15-CR-3134, 2016 WL 7428390, at *10 (D. Neb. Dec. 23, 2016) ("[T]he Fourth Amendment inquiry requires an analysis not only of the information obtained, but more fundamentally, the means of obtaining it."). Thus, "[a] phone conversation is private when overheard by means of a wiretap; but that same conversation is unprotected if an agent is forced to overhear it while seated on a Delta flight. Similarly, information that is not particularly sensitive—say, the color of a suspect's vehicle—might be protected if government agents broke into the suspect's garage to get it," but unprotected if observed while the car is driving on a public street. *Carpenter*, 819 F.3d at 888. So, too, might police "learn how many people are in a particular house by setting up year-round surveillance; but that does not make breaking and

entering to find out the same information lawful." *Kyllo v. United States*, 533 U.S. 27, 35 n.2 (2001).

Had the MPD *actually* located Defendant by tracking one of the stolen cell phones with the cell site simulator (pursuant to the consent of that phone's owner), the government might have argued that Defendant lacked a reasonable expectation of privacy in the information obtained. *See People v. Barnes*, 157 Cal. Rptr. 3d 853, 862 (Cal. Ct. App. 2013) ("[T]he use of GPS technology in ascertaining the location of the stolen cell phone, and thus assisting in the locating of defendant was no violation of the Fourth Amendment."). But that is not what happened here. The record indicates that the government actually located Defendant by using the cell site simulator to ensnare his own phone. The counterfactual supposition that he might have been located by tracking a stolen phone in his possession does not change the Fourth Amendment calculus. To the extent the Court is concerned with whether the MPD actually did or actually would have tracked and precisely located the stolen cell phones using the cell site simulator or other means, that question is best addressed within the framework of the inevitable discovery doctrine. *See infra* Part II.

The guiding principle here—that the constitutionality of a government search must be judged by how the government actually obtained the information in question, not how it might have otherwise obtained the same information from a

different source or by different means—is illustrated by the Supreme Court's landmark decision in *Riley v. California*, 134 S. Ct. 2473 (2014), which required a warrant for searches of cell phones incident to arrest. The government argued in that case that police should at least be permitted to access call logs on a cell phone without a warrant, citing the Supreme Court's decision in *Smith v. Maryland,* 442 U.S. 735 (1979). *Smith* "held that no warrant was required to use a pen register at telephone company premises to identify numbers dialed by a particular caller" because people have no reasonable expectation of privacy in information (dialed phone numbers) voluntarily shared with a third party (the phone company). *Riley*, 134 S. Ct. at 2492 (citing *Smith*, 442 U.S. at 745–46). The Court in *Riley* rejected the government's argument, holding that when police obtain call records through a search of the suspect's own cell phone, the Fourth Amendment requires a warrant, even if the same information properly could have been obtained without a warrant from another source. *Id.* at 2492–93.

Likewise, in *Kyllo v. United States*, the Court held that law enforcement agents must obtain a warrant before using a thermal imaging device to learn facts about the interior of a home, even if the same information could be obtained in other ways that do not require a warrant, "for example, by observing snowmelt on the roof." 533 U.S. at 35 n.2. The Court explained that "[t]he fact that equivalent information could sometimes be obtained by other means does not make lawful the

use of means that violate the Fourth Amendment." *Id.* The D.C. Circuit similarly concluded in *United States v. Maynard* that "when it comes to the Fourth Amendment, means do matter." 615 F.3d 544, 566 (D.C. Cir. 2010), *aff'd sub nom. United States v. Jones*, 565 U.S. 400 (2012). *Maynard* involved the prolonged GPS tracking of a suspect's car without a valid warrant. The court rejected the government's argument that because law enforcement agents could in theory have conducted uninterrupted visual surveillance of the suspect for 28 days, surreptitious GPS monitoring over that period did not implicate the Fourth Amendment. *Id.* at 565–66. The court applied the protections of the Fourth Amendment to the investigative means the government actually used, and concluded that the prolonged GPS tracking violated the Constitution. *Id.* at 566–67.

Courts have also held that the government violates a reasonable expectation of privacy when it obtains a suspect's internet protocol address by hacking into the suspect's computer and forcing the computer to transmit that information to the government. That is so even though courts generally agree that the people have no reasonable expectation of privacy in the IP addresses that they have shared with an internet service provider, and thus that the government can obtain the very same information from a service provider without a warrant. *See, e.g.*, *United States v. Croghan*, 209 F. Supp. 3d 1080, 1092 (S.D. Iowa 2016) ("There is a significant

difference between obtaining an IP address *from a third party* and obtaining it *directly from a defendant's computer*."); *United States v. Broy*, 209 F. Supp. 3d 1045, 1054 (C.D. Ill. 2016); *United States v. Darby*, 190 F. Supp. 3d 520, 529–30 (E.D. Va. 2016). As in *Riley* and the government hacking cases, the search here was of Defendant's own property—his phone itself—in which he clearly had a reasonable expectation of privacy. *See* Corrected Br. of the American Civil Liberties Union et al. as Amici Curiae, at 6 (citing *Riley*, 134 S. Ct. 2473). MPD's cell site simulator forced Defendant's cell phone to repeatedly transmit data stored on the phone—its unique electronic serial number—back to the government, which investigators used to home in on the phone's location. The fact that the MPD might properly have been able to search and locate other items in Defendant's possession without a warrant does not vitiate the Fourth Amendment's protections vis-à-vis a search of Defendant's phone.

B. Defendant's reasonable expectation of privacy is not diminished by the contraband nature of the stolen cell phones or the capability of the government to track those phones.

Neither the contraband nature of stolen goods nor the propensity of cell phones to broadcast information that renders them capable of being located diminishes the expectation of privacy here. It is black-letter law under the Fourth Amendment that possession of contraband does not diminish a person's reasonable expectation of privacy in an item or location for which a warrant is otherwise

required. Thus, "[e]ven 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. Jacobsen*, 466 U.S. 109, 114 (1984); *see also*, *e.g.*, *United States v. Chadwick*, 433 U.S. 1, 3–4, 15–16 (1977) (warrant required to search locked footlocker containing marijuana). It cannot be that possessing contraband goods, including stolen cell phones, vitiates the Fourth Amendment's protections against warrantless use of a cell site simulator.

The Fourth Amendment's application does not change if the contraband is capable of being located by government detection equipment or similar means. Imagine a driver with a trunk full of illegal drugs who is pulled over by police. If the officer searches the trunk without probable cause and discovers the drugs, she cannot justify the search on the basis that the odor of drugs wafting from the trunk *could have been* (but was not actually) detected by a drug-sniffing dog or its electronic equivalent. "Such a warrantless search could not be characterized as reasonable simply because, after the official invasion of privacy occurred, contraband is discovered." *Jacobsen*, 466 U.S. at 114. Likewise, if the officer located the driver by warrantlessly tracking his phone, she could not excuse the warrantless tracking by arguing that the drugs traveling with the driver were capable of being tracked and located by a drug-sniffing dog. The fact that

contraband could be, but was not in fact, located based on emanations or signals it produces does not render otherwise unconstitutional searches suddenly permissible.

A contrary ruling would prove a dangerous precedent in the digital age. The proliferation of electronic devices that travel with us as we go about our daily lives means that people will frequently be in possession of multiple devices that are independently trackable. Should the driver of a rental car with a GPS device installed by the rental company be susceptible to warrantless tracking of his cell phone on the theory that police could also request location information from the rental company? If a person accidentally leaves the house with both her own and her spouse's cell phones in her bag, should police be able to warrantlessly track her phone by reasoning that they could have sought consent of the spouse to track the spouse's phone? If a traveler has a wireless-internet-connected laptop issued by his employer and loaded with location-tracking software for use in case the device is stolen, can police track the traveler's personal cell phone without a warrant by claiming that they could have asked the employer to locate the laptop sitting in the same room? Any holding that permits warrantless use of a cell site simulator on a suspect's phone based on the presence of other potentially trackable items nearby would open a Pandora's box of exceptions to the warrant requirement. In order to prevent "police technology [from] erod[ing] the privacy guaranteed by the Fourth

Amendment," *Kyllo*, 533 U.S. at 34, this Court should hold that the use of a cell site simulator to surreptitiously track and locate a suspect's phone requires a valid warrant.

II. The Fourth Amendment implications of Defendant's possession of stolen cell phones are properly analyzed under the inevitable discovery doctrine, not the reasonable-expectation-of-privacy test.

The proper doctrinal framework for assessing the effect of Defendant's possession of stolen cell phones on his suppression motion is the inevitable discovery doctrine, not the reasonable-expectation-of-privacy test. If Defendant's possession of stolen cell phones that are capable of being located has any significance under the Fourth Amendment, it is on the question of whether police were in the process of actually tracking those phones, and whether they inevitably would have located one of the stolen devices even had the tracking of Defendant's own cell phone failed.

Considering as part of the reasonable-expectation-of-privacy inquiry the availability of alternative means to gather information would collapse inevitable discovery into the reasonable-expectation question in a manner that would radically transform both doctrines. As discussed above, a person's reasonable expectation of privacy is a function both of the information the government seeks and of the means it uses to obtain that information. This key protection, which the Supreme Court reaffirmed in *Kyllo* and *Riley*, would evaporate if factors relevant

to the inevitable discovery inquiry could be used to attack an expectation of privacy: The focus of the analysis would shift from what types of privacy expectations our society recognizes as reasonable to what types of theoretically-available-but-actually-unused means the government has at its disposal to invade those expectations. At the same time, the contours of the inevitable discovery doctrine, a carefully crafted exception to the exclusionary rule with strict requirements, *see* Br. for Appellant at 38–39, would be subject to end-runs, because the possibility of an alternative means of discovery could often be repackaged as a reason to reject an expectation of privacy in the first place. This Court's important admonition against the logic, "if we hadn't done it wrong, we would have done it right," *see* Reply Br. at 13, would be lost in translation.

Thus, analyzing this question in terms of the inevitable discovery doctrine will allow the Court to consider the particular course of the investigation in this case and the Defendant's entitlement to relief, without broadly undermining the protections of the Fourth Amendment in the digital age. Although amici take no position on the applicability of the inevitable discovery doctrine on these facts, they urge the Court to provide guidance on the Fourth Amendment's application to government use of cell site simulators regardless of whether suppression is warranted in this particular case. *See* Corrected Br. of the American Civil Liberties Union et al. as Amici Curiae, at 11–21.

May 10, 2017

Respectfully submitted,

/s/ Nathan Freed Wessler

Nathan Freed Wessler (*pro hac vice*) *
American Civil Liberties Union
Foundation
125 Broad Street, 18th Floor
New York, NY 10004
T: (212) 549-2500
F: (212) 549-2654
nwessler@aclu.org

/s/ Arthur B. Spitzer

Arthur B. Spitzer
Scott Michelman
American Civil Liberties Union
of the District of Columbia
4301 Connecticut Avenue, N.W.,
Suite 434
Washington, D.C. 20008
T: (202) 457-0800
F: (202) 457-0805
aspitzer@acludc.org

Jennifer Lynch
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
T: (415) 436-9333
jlynch@eff.org

*Counsel at Oral Argument

Certificate of Service

I hereby certify that I served a copy of the foregoing Supplemental Brief of American Civil Liberties Union, American Civil Liberties Union of the District of Columbia, and Electronic Frontier Foundation as Amici Curiae, using the Court's e-filing system, upon Stefanie Schneider, Public Defender Service for the District of Columbia, and Lauren Bates, Assistant United States Attorney, this 10th day of May, 2017.

/s/ Arthur B. Spitzer_____
Arthur B. Spitzer