No. 17-10230

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA

Plaintiff–Appellee,

v.

BRYAN GILBERT HENDERSON,

Defendant–Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE NORTHERN DISTRICT OF CALIFORNIA

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION, ACLU OF NORTHERN CALIFORNIA, ACLU OF ARIZONA, ACLU OF HAWAI'I & ACLU OF OREGON IN SUPPORT OF DEFENDANT–APPELLANT

Brett Max Kaufman
Vera Eidelman
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
T: 212.549.2500
F: 212.549.2654
bkaufman@aclu.org
veidelman@aclu.org

Jennifer S. Granick (CBN 168423)
American Civil Liberties Union Foundation
39 Drumm Street
San Francisco, CA 94111
T: 415.343.0758
jgranick@aclu.org

Additional counsel listed on next page

Linda Lye
American Civil Liberties Union
Foundation of Northern California
39 Drumm Street
San Francisco, CA 94111
T: 415.621.2493
F: 415.255.8437

Mateo Caballero
ACLU of Hawai‘i Foundation
P.O. Box 3410
Honolulu, HI 96801
mcaballero@acluhawaii.org

Kathleen E. Brody
ACLU Foundation of Arizona
3707 N. 7th Street, Suite 235
Phoenix, AZ 85014
T: 602.650.1854
kbrody@acluaz.org

Mathew dos Santos (OSB 155766)
ACLU Foundation of Oregon, Inc.
P.O. Box 40585
Portland, OR 97240
mdossantos@aclu-or.org

Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

Amici Curiae American Civil Liberties Union, ACLU of Arizona, ACLU of Hawai‘i, ACLU of Northern California, and ACLU of Oregon 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.*

/s/ Jennifer S. Granick

Jennifer S. Granick
American Civil Liberties Union
Foundation
39 Drumm Street
San Francisco, CA 94111
T: 415.343.0758
jgranick@aclu.org

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes and Rules

Other Authorities

INTEREST OF *AMICI CURIAE*[1]

The American Civil Liberties Union ("ACLU") is a nationwide, non-profit, non-partisan organization of more than 1.2 million members dedicated to defending the civil liberties guaranteed by the Constitution. The ACLU of Arizona, ACLU of Hawai'i, ACLU of Northern California, and ACLU of Oregon are geographic affiliates of the National ACLU. The ACLU has been at the forefront of numerous state and federal cases addressing the right of privacy as guaranteed by the Fourth Amendment.

[1] Pursuant to Rule 29(a)(2), counsel for *amici curiae* certifies that Defendant–Appellant Henderson and Plaintiff–Appellee United States consent to the filing of this amicus brief. In addition, counsel for *amici curiae* certifies that no counsel for a party authored this brief in whole or in part, and no person other than *amici curiae*, their members, or their counsel made a monetary contribution to its preparation or submission.

SUMMARY OF ARGUMENT

This case presents an important question about the role of judicial review in the digital age, when the government can attempt—as it did in this case—to use a single order issued by a single magistrate judge on the basis of insufficient and misleading information to search more than 8,700 computers in more than 120 countries around the world. The investigative technique used in this case, and close to 140 other criminal prosecutions around the country, was highly intrusive and involved serious risks to third parties. Left unchecked by courts like this one, the government's deployment of this technique threatens both the Constitution and the security of the Internet.

Because the government used novel surveillance technology in this prosecution, independent judicial evaluation of the warrant application required an understanding of complicated technological terms and processes. Yet, in applying for this novel and wide-reaching warrant, the government failed to disclose material facts to the magistrate judge. Specifically, the government failed to disclose that (1) the government would use malicious software that would force visitors' computers to malfunction in a way that could grant the government access to sensitive information outside the categories listed in the warrant, and wholly unrelated to the criminal investigation; and (2) the government's malware created security risks—of which the government was well aware—for millions of

innocent, non-targeted users. These omissions impaired the magistrate's ability to perform her duty of independent evaluation of the warrant's compliance with the Fourth Amendment, and her duty to ensure that the government took necessary steps to safeguard innocent third parties. For the reasons set forth in Defendant–Appellant's brief, as well as those set forth below, suppression is appropriate.

FACTUAL STATEMENT

This case arises from the government's use of malicious software ("malware") to hack into thousands of computers by breaking through an anonymity- and security-providing network called "Tor" to unmask visitors to a website called "Playpen."

I. Government Hacking

More and more, the FBI relies on malware to collect information that is transmitted by or stored on anonymous targets' computers. (The term "malware" refers to software which is intended to covertly damage a computer system or its data, and/or to take partial control of its operation.[2])

[2] Malware, Dictionary.com, http://www.dictionary.com/browse/malware (last visited Oct. 31, 2017). The U.S. National Institute of Standards and Technology formally defines malware as "a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system." Murugiah Souppaya and Karen Scarfone, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops, Nat'l Inst. of Standards and Tech. Special Publ'n* 33 (2013), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

The government has been using malware to target specific, individual anonymous suspects since at least 2002.[3] More recently, the FBI has expanded from the tailored deployment of malware against individual targets to "watering hole" operations, in which the FBI delivers malware to all individuals who visit a particular website.

The FBI is known to have conducted watering hole operations in at least three investigations of child pornography sites. One involved delivery of malware to visitors to multiple websites hosted by Freedom Hosting. As explained more fully below, while some of these sites hosted child pornography, others had nothing to do with illegal activity. The FBI deployed its malware too broadly, infecting innocent Internet users.[4] The most recent publicly known malware investigation is the one at issue in this case, aimed at users of Playpen.[5]

---

[3] Kevin Poulsen, *Documents: FBI Spyware Has Been Snaring Extortionists, Hackers For Years*, Wired, Apr. 16, 2009, https://www.wired.com/2009/04/fbi-spyware-pro.

[4] Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, Wired, Sept. 19, 2013, https://www.wired.com/2013/09/freedom-hosting-fbi.

[5] Cyrus Farivar, *After FBI Briefly Ran Tor-Hidden Child-Porn Site, Investigations Went Global*, Ars Technica, Jan. 22, 2016, http://arstechnica.com/tech-policy/2016/01/after-fbi-briefly-ran-tor-hidden-child-porn-site-investigations-went-global.

II. Tor

Playpen was only available to computers that used Tor. Tor is a freely available form of computer privacy protection—a network that exists to "enable users to communicate privately and securely"[6] by protecting a user's Internet Protocol ("IP") address,[7] location, and usage from hacking or disclosure. The U.S. government originally created Tor, which serves as an essential tool for activism and free speech across the world.[8] Journalists, bloggers, whistleblowers, human rights workers, and other activists have relied on the Tor network to avoid surveillance by potentially repressive regimes.[9]

---

[6] Tor Project, *Statement from the Tor Project re: the Court's February 23 Order in U.S. v. Farrell*, Tor Blog (Feb. 24, 2016), https://blog.torproject.org/statement-tor-project-re-courts-february-23-order-us-v-farrell.

[7] An IP address is a string of zeros and ones that identifies a machine that is connected to the Internet, and which is used to route messages to that machine. Unlike a "MAC" address, which, as described further below, is unique and static, an IP address is not permanent and one machine could have more than one IP address over its lifetime—or even at a given time. *See Why Does Your IP Address Change Now and Then?*, WhatIsMyIPAddress.com, http://whatismyipaddress.com/keeps-changing (last visited Oct. 31, 2017).

[8] Yasha Levine, *Almost Everyone Involved in Developing Tor Was (or Is) Funded by the US Government*, Pando, July 16, 2014, https://pando.com/2014/07/16/tor-spooks; see also *Our Sponsors*, Onion Routing, https://www.onion-router.net/Sponsors.html (last visited Oct. 31, 2017); *United States v. Knowles*, No. CR 2:15-875-RMG, 2016 WL 6952109, at *2 (D.S.C. Sept. 14, 2016) ("The Department of Defense designed Tor to protect government communications").

[9] Tor Project, *Users of Tor: Inception*, https://www.torproject.org/about/torusers.html.en (last visited Oct. 31, 2017).

Using Tor is relatively easy, and millions of people do so. *See* Tor Project, *Tor Metrics*, https://metrics.torproject.org. To use Tor, individuals need only download a special web browser based on the popular Firefox browser.10 After installation, the Tor browser automatically establishes an anonymous, encrypted connection. To do this, Tor employs a series of volunteer computers or "relay nodes" to transmit each connection request. The original data is encrypted in such a way that only the last (or "exit") relay can decrypt it. That bundle, in turn, is encrypted in such a way that only the relay right before the exit relay can decrypt it, and so on, in layers, all the way to the first (or "entry") relay. As a result, no single server in the Tor network can trace a user's path through the network to the requested site.

III. Government Operation of Playpen and the Search Warrant

The government became interested in Playpen upon learning that unknown individuals were using the website to distribute and obtain child pornography. On February 19, 2015, the government took over the site and ran it for 15 days.

On February 20, 2015, the government submitted an application and affidavit for a search warrant to a magistrate judge in the Eastern District of Virginia. ER II 72. In the affidavit, the government told the magistrate judge that it

[10] Tor Project, *What is Tor Browser*?, https://www.torproject.org/projects/torbrowser.html.en (last visited Oct. 31, 2017).

would move the seized Playpen website to a government-controlled computer server in Virginia and that the website "will continue to operate from the government-controlled computer server." ER II 147, ¶ 52.

It would not have been obvious to a visitor to the Playpen homepage that the site contained contraband images. Indeed, the site included subdirectories and forums that did not contain child pornography or any other illegal materials. *See* Motion and Memorandum In Support Of Motion To Dismiss Indictment (hereinafter "*Michaud* Motion") at 2–3, *United States v. Michaud*, No. 15-cr-05351-RJB (W.D. Wash. Nov. 20, 2015), ECF No. 50 (discussing Playpen's "fiction," "artwork," and chat sections); *see also United States v. Gourde*, 440 F.3d 1065, 1070 (9th Cir. 2006) (recognizing that child erotica and adult pornography are legal content). Nevertheless, the warrant application broadly sought to deploy the malware as follows:

> During the up to thirty day period that the NIT is deployed on the TARGET WEBSITE, . . . each time that any user or administrator logs into the TARGET WEBSITE by entering a username and password, this application requests authority for the NIT authorized by this warrant to attempt to cause the user's computer to send the above-described information to a computer controlled by or known to the government that is located in the Eastern District of Virginia.

ER II 101, ¶ 36 (emphases added).

While the government indicated that it might choose to deploy the malware in a more targeted fashion at its discretion, it sought authorization

to deploy the malware to investigate "any user" who logged into the site's home page, regardless of their physical location and whether or not they were engaged in only lawful conduct. ER II 99, ¶ 33 n. 8.

IV. The Government's Malware

Because Playpen was only available through Tor, which masked the IP addresses of Playpen visitors, the FBI decided to use malware to force the visitors' computers to disclose their IP addresses and other identifying information.

Instead of using the term "malware" in applying for the warrant here, however, the government used a sterilized term—"Network Investigative Technique," or "NIT"—which is not generally used in computer science.[11] Presumably, NIT is the government's term for technology that is deployed through a watering hole attack rather than in a targeted fashion.

In this case, the government's malware consisted of two important pieces: a "payload," computer code that instructed each computer that visited Playpen to

[11] *See, e.g.*, Joseph Cox, *The FBI Used a 'Non-Public' Vulnerability to Hack Suspects on Tor*, Motherboard, Nov. 29, 2016, https://motherboard.vice.com/en_us/article/kb7kza/the-fbi-used-a-non-public-vulnerability-to-hack-suspects-on-tor ("In February 2015, the FBI seized dark web child pornography site Playpen, and used *what the agency calls* a network investigative technique (NIT)—*a piece of malware*—to break into suspected visitor's computers and learn their real IP address." (emphasis added).

send identifying information back to the government, and an "exploit,"[12] which delivered the payload. The exploit was necessary to force the users' browsers to download and run the payload. Though the precise functionality of the exploit is not publicly known because the government refuses to disclose the NIT's source code, it is known that the exploit consisted of software that broke certain aspects of the visitors' browsers. Specifically, the exploit took advantage of a flaw in the Tor browser, bypassing security measures that exist to prevent a hostile website from taking over a user's machine.[13]

The exploit's potential for harm and intrusiveness was significant: it was capable of taking total control of a user's computer. *See* Mozilla's Motion To Intervene Or Appear As Amicus Curiae In Relation To Government's Motion For Reconsideration Of Court's Order On The Third Motion To Compel (hereinafter "Mozilla Motion") at 9–10, *United States v. Michaud*, No. 15-CR-05351-RJB (W.D. Wash. May 11, 2016), ECF No. 195 (the exploit "allows a third party to tell

[12] See, e.g., *Windows Defender Security Intelligence*, Microsoft, https://www.microsoft.com/en-us/wdsi/threats/exploit-malware (last visited Oct. 31, 2017) ("Exploits take advantage of weaknesses of 'vulnerabilities' in common software . . . Malware can use these vulnerabilities to exploit the way software works and further infect your [computer]."); *Viruses, Worms, Trojans, and Bots,* Cisco, https://www.cisco.com/c/en/us/about/security-center/virus-differences.html#9 (last visited Oct. 31, 2017) ("An exploit is a piece of software, a command, or a methodology that attacks a particular security vulnerability . . . [T]hey are a common component of malware.").

[13] Declaration of Brian N. Levine, Ph.D. at ¶ 4, *United States v. Tippens*, No. 16-cr-5110-RJB (W.D. Wash. Sept. 22, 2016), ECF No. 58-1.

the computer to run its code, instead of what the computer should run next. Once this happens, the third party can gain total control of the computer."). This means the "third party can see what the user is doing in a different browser tab, read all data on the computer, see every action the user takes or even turn on the computer's camera or microphone to watch and listen to the user." *Id.* at 9. Because the Tor browser is based on Firefox, the government's exploit code could be used not only to affect Tor's million users, but also to compromise the computer security of Firefox's several hundred million users. Mozilla Press Center, *Mozilla at a Glance*, https://blog.mozilla.org/press/ataglance; *see also* Mozilla Motion at 2–3.

ARGUMENT

I. The Government Has a Fourth Amendment Duty To Be Honest and Forthcoming With the Magistrate Judge so She Can Fulfill Her Constitutionally Mandated Role.

In order to ensure that the search in this case would comply with the Fourth Amendment, including its "general touchstone of reasonableness," *United States v. Ramirez*, 523 U.S. 65, 71 (1998), the magistrate judge needed to know all relevant facts going to probable cause, particularity, and the risks to third parties from the search's execution. *See United States v. Hillyard*, 677 F.2d 1336, 1339 (9th Cir. 1982); *VonderAhe v. Howland*, 508 F.2d 364, 370 (9th Cir. 1974). The Supreme Court has emphasized "[o]ver and again" that searches conducted "without prior

approval by judge or magistrate, are per se unreasonable under the Fourth Amendment." *Katz v. United States*, 389 U.S. 347, 357 (1967) (alteration and quotation marks omitted). Judicial review is "[t]he bulwark of [the] Fourth Amendment," *Franks v. Delaware*, 438 U.S. 154, 164 (1978), as judges are "charged with upholding" the "safeguards of the Fourth Amendment" by independently evaluating warrant applications. *United States v. Rettig*, 589 F.2d 418, 422 (9th Cir. 1978).

When it comes to government's use of novel surveillance technology, the court needs basic information about what the technology is and how it effectuates the search. This information is necessary to ensure that the court can execute its constitutional duty of supervising the search to ensure it complies with the Fourth Amendment's requirements of probable cause, particularity, and reasonableness.

In order for a court to ensure that the government does not violate the Fourth Amendment, "[a]n officer presenting a search warrant application has a duty to provide, in good faith, all relevant information to the magistrate." *United States v. Perkins*, 850 F.3d 1109, 1116 (9th Cir. 2017) (citing *United States v. Hill*, 459 F.3d 966, 971 n.6 (9th Cir. 2006)). A magistrate cannot "'mere[ly] ratif[y] . . . the bare conclusions of others,'" *id.* (quoting *Illinois v. Gates*, 462 U.S. 213, 239 (1983)), rather, the government must present her with sufficient information to "make an independent evaluation of the matter." *Id.* (quoting *Franks*, 438 U.S. at 165); *see*

also United States v. Comprehensive Drug Testing, Inc. (*CDT*), 621 F.3d 1162, 1178 (9th Cir. 2010) (en banc) (Kozinski, J., concurring) ("A lack of candor in . . . any . . . aspect of the warrant application must bear heavily against the government in the calculus of any subsequent motion to return or suppress the seized data.").

Moreover, magistrates must consider whether proposed searches pose indiscriminate risks to third parties or are unduly excessive in their means. To that end, courts must consider whether technology used to execute a search is simply too dangerous.

Deployment of technology to conduct searches that are overbroad, or pose excessive risk to life or property are unreasonable. Absent specific safeguards, "inherently dangerous" law enforcement techniques that are likely to harm innocent bystanders fail the Fourth Amendment's reasonableness requirement. This Court has held that use of a flashbang device in an apartment violates the Fourth Amendment's reasonableness requirement and thereby constitutes excessive force when innocent third parties could be sleeping inside. *Boyd v. Benton Cty.*, 374 F.3d 773, 779 (9th Cir. 2004); *see also Bing ex rel. Bing v. City of Whitehall*, 456 F.3d 555, 570 (6th Cir. 2006) ("[E]mploy[ing] a flashbang device [to enter a house] with full knowledge that it will 'likely' ignite accelerants and cause a fire" is unreasonable under the Fourth Amendment.). Similarly, the California Supreme Court has held that, absent judicial review and exigent

circumstances, using a motorized battering ram to enter homes fails the Fourth Amendment's reasonableness requirement because of the ram's potential to break walls, ceilings, and utility lines, which "threaten[s] the safety not only of occupants, but of entire neighborhoods." *Langford v. Superior Ct. of L.A. Cty.*, 43 Cal. 3d 21, 29 (Cal. 1987).

Needless to say, to make such an assessment, the magistrate needs to be informed of and understand the technology the government plans to use to enter a suspect's premises—whether it is a flashbang grenade, a battering ram, or malware that threatens computer security.

If the government's recitation of the facts is "incomplete and misleading," it "effectively usurp[s] the magistrate's duty to conduct an independent evaluation." *Perkins*, 850 F.3d at 1118. In *Perkins*, this Court expressly recognized the duty the affiant owes to the magistrate, and its critical connection to the magistrate's independent evaluation of a warrant's compliance with the Fourth Amendment. 850 F.3d at 1116–19. The Court held that "an incomplete and misleading recitation of the facts and . . . [certain] images" prevents a magistrate from doing her constitutionally mandated job. *Id.* at 1118 (emphasis omitted).

In that regard, omissions may be just as fatal and misleading as affirmative misrepresentations. That is because the magistrate can only evaluate the constitutionality of a warrant application "based on the information that was

actually provided to him." *United States v. Lull*, 824 F.3d 109, 116 (4th Cir. 2016) (holding that suppression was warranted where the investigator omitted details from his affidavit). This Court has "recognized that an affiant can mislead a magistrate '[b]y reporting less than the total story, [thereby] . . . manipulat[ing] the inferences a magistrate will draw.'" *Perkins*, 850 F.3d at 1117–18 (quoting *United States v. Stanert*, 762 F.2d 775, 781 (9th Cir. 1985), *amended by* 769 F.2d 1410 (9th Cir. 1985)). "To allow a magistrate to be misled in such a manner could denude the [Fourth Amendment's] requirement[s] of all real meaning." *Stanert*, 762 F.2d at 781.

Moreover, as this Court has recognized, computer searches like the one at issue here are uniquely challenging to keep within the boundaries of the Fourth Amendment. *United States v. Tamura*, 694 F.2d 591, 595–97 (9th Cir. 1982). The enormous capacity and fast data-transfer capabilities of modern digital devices elevate the danger that warrants for electronic searches, if not carefully circumscribed, will turn into the general warrants that the Fourth Amendment was specifically adopted to prohibit. *See CDT*, 621 F.3d at 1168–69, 1176 (*per curiam*); *id.* at 1180 (Kozinski, J., concurring) (discussing the heightened risk of "over-seizing of evidence" during digital searches); *United States v. Payton*, 573 F.3d 859, 862 (9th Cir. 2009) ("Searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from

searches of other containers. Such considerations commonly support the need specifically to authorize the search of computers in a search warrant."). And because so many intimate details reside on digital devices, such searches will not only implicate a device's owner, but third parties as well. *See, e.g.*, *In re U.S.'s Application for a Search Warrant to Seize & Search Elec. Devices from Edward Cunnius*, 770 F. Supp. 2d 1138, 1144 (W.D. Wash. 2011).

In such contexts, "it is self-evident that the court must understand why and *how* the search is to be conducted . . . The analytical framework requires analysis of the functionality of the surveillance device and the range of information potentially revealed by its use." *Maryland v. Andrews*, 134 A.3d 324, 338 (2016) (emphasis in original). Judges can only fulfill their constitutional role if law enforcement fully and candidly discloses all relevant facts in search warrant applications—an obligation the government failed to satisfy in this case.

II. The Government Failed its Duty To Be Honest and Forthcoming With the Magistrate Judge About Relevant Facts Regarding the Playpen Investigation.

Here, the government failed to fully disclose critical information to the magistrate judge. The government omitted or misrepresented several facts that the government possessed but chose not to disclose. First, the government did not inform the magistrate that the NIT included exploit code. Nor did it tell the court that the exploit code would cause the users' browsers to malfunction and thereby

allow the government, or any attacker who used the exploit, to download whatever software it wished to the device. By keeping the exploit secret, the government failed to disclose the risk that its malware could result in overbroad searches. Second, the government failed to fully set forth the potential of the exploit-dependent search to endanger third parties—including innocent Tor and Firefox users—and the security of the entire Internet more generally. As in *Perkins*, all of these omissions combined to result in the government "effectively usurp[ing] the magistrate's duty to conduct an independent evaluation" of probable cause, particularity, scope of the search, and general reasonableness under the Fourth Amendment, thereby rendering the search unconstitutional.[14]

A. The Government Failed to Disclose That the Malware's Exploit Code Created a Risk That the Government's Computer Searches Would Be Overbroad.

The Playpen warrant application obfuscated the risk that the government would acquire sensitive information outside of the seven categories listed in the warrant, even if by accident. As noted above, this Court has recognized the particular intrusiveness of computer searches and has urged caution in issuing warrants targeting computers due to the risk of "over-seizing" evidence. *CDT*, 621

[14] In addition to the issues highlighted herein, *amici* agree with Appellant that the government masked the fact that its NIT would search computers outside of the district, thereby violating Federal Rule of Criminal Procedure 41 and justifying suppression.

F.3d at 1177. The government's failure here to disclose the existence and operation of an important piece of its malware—the "exploit"—violated this admonition. The warrant mentioned one piece of the malware—the "payload" (i.e., what the NIT would place on the computers)—but not the other piece—the "exploit" (i.e., how it would do so). This exploit likely gave the government total, and at the very least significant, control over infected computers. By failing to mention it, the government omitted critical information concerning the scope of the computer search's intrusiveness from the magistrate.

Exploit code can give government agents expansive access to a user's computer. Here, the exploit forced the user's browser to malfunction. Though the government refuses to disclose the precise exploit it used, *see* Government's Unopposed Motion to Dismiss Indictment Without Prejudice, *United States v. Michaud*, No. 15-cr-05351-RJB (W.D. Wash. Mar. 3, 2017), ECF No. 227, it has acknowledged that the exploit was able to force the computer to download and run the government's payload code. ER II 101, ¶ 36.

The ability to bypass browser security and force a computer to download and run computer instructions hidden in a webpage is extremely powerful. Once the government uses the exploit, it is able to "tell the computer to run its code, instead of what the computer should run next." Mozilla Motion at 9–10. If Mozilla is correct about the nature of the exploit used in this case, after delivering the

exploit, the government could have accessed anything on the malfunctioning computer—stored documents, photos, and more. It could also have logged a user's keystrokes, enabling the government to obtain passwords, read email drafts, and track browsing history. It could enable real-time monitoring of video calls, something for which the government would need a wiretap order. It could record other network traffic, such as the domain names that the computer looks up and where it sends traffic. It could gain access to encrypted files in unencrypted form without ever learning a password. The exploit gave the government each of these capabilities, and yet the government left the fact of the exploit's existence out of its application entirely

In computer searches where the government can access the private data intermingled with data for which there is probable cause, the magistrate has an important role to play in monitoring the government's conduct both before and after the search so that it does not run afoul of the Fourth Amendment. *See CDT*, 621 F.3d at 1178 (Kozinski, J., concurring). But here, the magistrate was not told that the government was using an exploit with expansive capabilities to acquire sensitive information outside of the seven categories listed in the warrant and wholly unrelated to the criminal investigation, even if by accident.

Without knowing that the government was using an exploit to access users' machines, the magistrate was prevented from working with the government to

ensure compliance with the Fourth Amendment. As Judge Kozinski explained in *Comprehensive Drug Testing*, magistrate judges should exercise their warrant-oversight powers by ensuring that the government's access is limited to retrieving information responsive to the warrant (and *particularly* supported by probable cause). *See id*. By failing to address the full capabilities of the malware used in this case, the government's affidavit presented the magistrate with only a partial view of what was at stake.

If the magistrate judge had had reason to know that this kind of vigilance might be required, she might have imposed on the government one or more of the recommendations identified in *Comprehensive Drug Testing*. For example, she might have asked the FBI to waive reliance on the plain view doctrine; insisted that the payload data be segregated and redacted by specialized personnel or an independent third party to ensure that officers would not benefit from unavoidably overbroad searches; scrutinized closely the payload's operation to ensure that it was designed to uncover only the information for which the government had probable cause; and/or required the government to destroy non-responsive data or data that it would not use in a criminal investigation. *Id.* at 1179. Because the government refused to fully explain how the malware worked, it prevented the magistrate judge from understanding the full scope of what the malware was going to do, and prevented her from assessing whether the government was doing enough

to limit the data that the malware collected on the activating computers. The government's failure necessarily impaired the magistrate's duties to independently evaluate the warrant application and to supervise the search. *Perkins*, 850 F.3d at 1116; *CDT*, 621 F.3d at 1178; *Rettig*, 589 F.2d at 423 (ordering suppression where government's omissions deprived court of opportunity to craft "explicit limitations . . . to prevent an overly intrusive search.").

B. The Government Failed to Disclose That It Intended To Use Malware That Created Inherent Security Risks to Innocent, Non-Targeted Users.

The government's use of exploit code also posed risks that the search would violate the Fourth Amendment by impacting innocent third parties, but the government's failure to disclose those risks prevented the magistrate from considering the imposition of relevant protections. The need to include such protections in electronic surveillance orders is well established. *See, e.g.*, *Berger v. New York*, 388 U.S. 41, 59–60 (1967) (explaining need for limits on wiretap orders to avoid overbroad collection); *CDT*, 621 F.3d at 1176–77 (*per curiam*) (discussing importance of limiting instructions in search warrants for electronic data to protect the privacy of third parties); *In re Application of the U.S. for an Order Pursuant to 18 U.S.C. §§ 2703(C) & 2703(D) Directing AT&T, Sprint/Nextel, T-Mobile, MetroPCS and Verizon Wireless to Disclose Cell Tower Log Information*, 42 F. Supp. 3d 511, 519 (S.D.N.Y. 2014) (conditioning grant of order for cell tower

dump records on sufficiency of "protocol to address how the Government will handle the private information of innocent third-parties whose data is retrieved."); *see also* 18 U.S.C. § 2518(5) (requiring minimization of collection of non-pertinent conversations through a wiretap). But here, the magistrate judge could not have known to address these risks because of the government's failure to disclose them.

The government's use of malware poses unique risks because of the possibility that the government will lose control of the malware—whether because an insider leaks or sells the tools, because the government is hacked, or because a malware target identifies and publishes the code. Once a hacking tool has been disclosed outside the government, malicious actors have a window of opportunity to use it for their own nefarious purposes.

This risk is not theoretical. In fact, the wider the net the government casts—here it sought to serve as many as 158,000 computers with this malware—the more likely it is to lose control of the malware. That is because any one of the individuals visiting a target site could identify the fact that the site is distributing malware, save the code, analyze it, and publish it. This has happened before. In 2013, the FBI deployed malware on multiple websites hosted by Freedom Hosting. Like the malware at issue here, the Freedom Hosting malware took advantage of a Firefox security vulnerability to identify users of Tor. Innocent individuals who visited the targeted sites—which included legal content, including an encrypted

email service known as TorMail[15]—noticed the hidden computer instructions embedded in the sites and, within days, the code was being "circulated and dissected all over the net."[16] Researchers were able to learn how the exploit worked, and also to correctly guess that the FBI had designed the malware.

Freedom Hosting is not the only, or the most dangerous, example of the government losing control of exploit code. In 2016, the public learned that an entity calling itself the "Shadow Brokers" obtained National Security Agency ("NSA") malware. Following some initial attempts to sell the exploits, the Shadow Brokers dumped dozens of NSA hacking tools online for free in April 2017.[17] And in March 2017, a leak exposed thousands of pages of Central Intelligence Agency ("CIA") records documenting some of the CIA's hacking exploits,[18] including an exploit for a critical vulnerability in common routers and switches.[19]

---

[15] Ellen Nakashima, *This Is How the Government Is Catching People Who Use Child Porn Sites*, Wash. Post, Jan. 21, 2016, http://wpo.st/_lRh1.

[16] Kevin Poulsen, *Feds Are Suspects In New Malware That Attacks Tor Anonymity*, Wired, Aug. 5, 2013, https://www.wired.com/2013/08/freedom-hosting.

[17] Bruce Schneier, *Who Are the Shadow Brokers?*, The Atlantic, May 23, 2017, http://theatln.tc/2gSc3yQ.

[18] Scott Shane, Matthew Rosenberg & Andrew W. Lehren, *WikiLeaks Releases Trove of Alleged C.I.A. Hacking Documents*, N.Y. Times, Mar. 7, 2017, http://nyti.ms/2gRIo8M.

[19] *See id.*

When the government loses control of these exploits, businesses and human lives are endangered. One of the tools the Shadow Brokers released exploited a flaw in Microsoft software. Once it was released, others on the Internet repurposed the tool into a virulent piece of ransomware that infected hundreds of thousands of computer systems worldwide in May 2017.[20] The very next month, another malware attack combined that same tool with another NSA exploit released by the Shadow Brokers. After initially hitting critical infrastructure in Ukraine, that attack began spreading internationally and infected hospitals, power companies, shipping companies, and the banking industry, endangering human life as well as economic activity.[21]

The government is aware of the risk of losing control of its malware. In opposing a Freedom of Information Act request, the government cited this risk to prevent disclosure of which company sold it an exploit to unlock the iPhone used by one of the attackers in San Bernardino in 2015. The government argued, and the court agreed, that disclosure could put the company at risk of being hacked, and the sensitive malware of getting stolen. Josh Gerstein, *Judge: FBI Can Keep Cost*

---

[20] Bill Brenner, *WannaCry: The Ransomware Worm That Didn't Arrive on a Phishing Hook*, Naked Security, May 17, 2017, https://nakedsecurity.sophos.com/2017/05/17/wannacry-the-ransomware-worm-that-didnt-arrive-on-a-phishing-hook.

[21] *NHS Cyber-Attack: GPs and Hospitals Hit by Ransomware*, BBC News, May 12, 2017, http://www.bbc.com/news/health-39899646.

of iPhone Hack Secret, Politico, Oct. 1, 2017, http://www.politico.com/blogs/under-the-radar/2017/10/01/judge-fbi-need-not-release-cost-of-iphone-hack-243338. Yet in this case, the government said nothing.

This case and the incidents above make clear not only that the government may well lose control of malware, but also that the resulting damage to innocent parties' computer systems—and to the businesses and individuals that depend on these systems—is significant. A fully apprised magistrate could have inquired into the means the government was using to keep its exploit secure from unauthorized access. Instead, kept in the dark, the magistrate had no opportunity to assess and avoid the risk to innocent people, as the Constitution requires. *Perkins*, 850 F.3d at 1116.

C. Malware Searches That Exploit Vulnerabilities in Commonly Used Software Are So Risky That They Are *Per Se* Unreasonable or At Least Require Safeguards Beyond a Mere Warrant.

The magistrate judge should have been apprised of the malware's invasive and destructive nature not only for the reasons listed above, but also to enable her to assess whether such malware-based searches can be reasonable under the Fourth Amendment. The risk that this exploit posed to millions of lawful Tor and Mozilla users made the search *per se* unreasonable.

Sometimes, the technology used to execute a search is simply too dangerous to satisfy the Constitution. Absent specific safeguards, "inherently dangerous" law

enforcement techniques that threaten third parties are unreasonable under the Fourth Amendment, even where a warrant was issued. For example, in *Boyd v. Benton County*, this Court considered a search conducted with a warrant, but only after law enforcement used a flash bang grenade to enter the targeted premises. This Court held that, notwithstanding the existence of the warrant, the force used to conduct the search rendered the government's conduct unreasonable under the Fourth Amendment. 374 F.3d at 779. Similarly, in *Langford v. Superior Court of Los Angeles County*, the Supreme Court of California held that using a battering ram to enter dwellings was unconstitutional without advance judicial authorization *and* exigent circumstances because of the risk it posed to the structures—walls, ceilings, and utility lines—of third parties. 43 Cal. 3d at 233. The use of malware in this case is of a piece with these presumptively unreasonable techniques. As discussed above, it threatened the security of millions of computers.

Alternatively, the magistrate judge should have required more than probable cause before authorizing the malware search. Where an investigative technique is particularly invasive of privacy, the Supreme Court has required more than a search warrant. For example, in *Berger*, 388 U.S. 41, the Court considered what the Fourth Amendment requires a magistrate to find to lawfully authorize eavesdropping. The Court explained that because eavesdropping "by its very nature . . . involves an intrusion on privacy that is broad in scope," the issuing

court has "a heavier responsibility" when assessing such searches for "particularity and evidence of reliability." *Id.* at 56. The Court thus required that, *in addition to* probable cause, a valid wiretap order should be supported by a heightened level of particularity, including identification of the crime and the conversations to be overheard, as well as limits on the time period for executing the search, notice to affected parties, and a return on the warrant. *Id.* That is why the Wiretap Act, passed a year after *Berger* and written to conform to the constitutional requirements set out in *Berger* and *Katz*, 389 U.S. 347, imposes safeguards on wiretapping beyond those required for issuance of a run of the mill warrant. *See* 18 U.S.C. § 2510 *et seq*., S. Rep. No. 1097, 90th Cong., 2d Sess., 1968 U.S.C.C.A.N. 2112 (1968). As the Court found in *Berger*, the magistrate assessing the NIT in this case should have made a thorough, searching inquiry into probable cause and particularity, and imposed additional constitutional safeguards. The government's failure to disclose the existence of the exploit and the full reach of the malware robbed the magistrate judge of this opportunity to fulfill her duty.

D. No Exigent Circumstances Justified This Exploit-Based Search Since the Government Had the Information Necessary to Execute a Narrower, More Targeted Search of Specific Suspects.

The government had alternative means of identifying individuals engaged in illegal activity on Playpen and could have avoided the risks associated with malware searches. The government controlled the Playpen server and so could

track the user names of Playpen's 158,000 visitors and gather detailed data about their activities, such as the specific pictures or videos they viewed. *See* Defendant–Appellant's Opening Brief at 32-34, *United States v. Henderson*, No. 17-10230 (9th Cir. Oct. 24, 2017) ECF No. 8 (citing ER II 90-95, ¶¶ 14–27.) The government also obtained a wiretap warrant that permitted it to intercept chat conversations taking place on the site. ER II 107, 122-23, ¶¶ 8–9. Using that specific, individualized information, the government could have tried to identify particular users and sought warrants based on particularized facts. See Defendant–Appellant's Opening Brief, *Henderson,* at 34. But the government chose not to take that approach.

Instead, the government took a bulk approach, seeking a warrant to infect *anyone* who logged into the site with a username and password—including individuals who were accessing lawful content. ER II 88-89, ¶ 12. As noted above, the site's homepage was not designed to make it obvious that Playpen contained illegal images. And the site in fact offered lawful content, including fiction, artwork, chat, and child erotica sections. *See Michaud* Motion at 1070. Because the government did not explain to the court how much it knew about the Playpen users it was actually interested in, the magistrate was not in a position to assess whether the government could and should more narrowly tailor its search, including deployment of the malware.

CONCLUSION

As delineated above, the government omitted many critical facts from the warrant application. "By providing an incomplete and misleading recitation of the facts . . . [the government] effectively usurped the magistrate's duty to conduct an independent evaluation of probable cause." *Perkins*, 850 F.3d at 1118. The magistrate's independent and neutral role of evaluating overbreadth and intrusiveness in the execution of the search and risks to innocent third parties was undermined by these misrepresentations and omissions such that the magistrate could not fulfill her constitutional duty. Accordingly, this Court should reverse the court below.

Respectfully submitted this 31st day of October, 2017.

/s/ Jennifer S. Granick

Jennifer S. Granick (CBN 168423)
American Civil Liberties Union Foundation
39 Drumm Street
San Francisco, CA 94111
T: 415.343.0758
jgranick@aclu.org

Brett Max Kaufman
Vera Eidelman
American Civil Liberties Union Foundation
125 Broad Street, 18th Floor
New York, NY 10004
T: 212.549.2500
F: 212.549.2654
bkaufman@aclu.org
veidelman@aclu.org

Linda Lye
American Civil Liberties Union
Foundation of Northern California
39 Drumm Street
San Francisco, CA 94111
T: 415.621.2493
F: 415.255.8437

Mateo Caballero
ACLU of Hawai‘i Foundation
P.O. Box 3410
Honolulu, HI 96801
mcaballero@acluhawaii.org

Kathleen E. Brody
ACLU Foundation of Arizona
3707 N. 7th Street, Suite 235
Phoenix, AZ 85014
T: 602.650.1854
kbrody@acluaz.org

Mathew dos Santos (OSB 155766)
ACLU Foundation of Oregon, Inc.
P.O. Box 40585
Portland, OR 97240
mdossantos@aclu-or.org

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

1. This brief complies with type-volume limits because, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(f), it contains 6,406 words.

2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type-style requirements of Federal Rule of Appellate Procedure 32(a)(6) because it has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in 14-point Times New Roman.

Dated: October 31, 2017

/s/ Jennifer S. Granick

Jennifer S. Granick
American Civil Liberties Union Foundation
39 Drumm Street
San Francisco, CA 94111
T: 415.343.0758
jgranick@aclu.org

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 31st day of October, 2017, the foregoing Brief of *Amici Curiae* American Civil Liberties Union, et al., was filed electronically through the Court's CM/ECF system. Notice of this filing will be sent by email to all parties by operation of the Court's electronic filing system.

/s/ Jennifer S. Granick
Jennifer S. Granick