No. 17-30117

UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA

Plaintiff–Appellee,

v.

DAVID TIPPENS,

Defendant–Appellant.

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF WASHINGTON, TACOMA DIVISION

BRIEF OF *AMICI CURIAE* AMERICAN CIVIL LIBERTIES UNION & ACLU OF WASHINGTON IN SUPPORT OF DEFENDANT-APPELLANT

Jennifer S. Granick
(CA Bar No. 168423)
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
jgranick@aclu.org
bkaufman@aclu.org
veidelman@aclu.org

Nancy L. Talner
(WA Bar No. 11196)
ACLU-WA Foundation
Shankar Narayan
(WA Bar No. 31577)
ACLU-WA
901 Fifth Ave., Suite 630
Seattle, WA 98164
(206) 624-2184
talner@aclu-wa.org
snarayan@aclu-wa.org

Karin D. Jones
(WA Bar No. 42406)
Stoel Rives LLP
600 University Street, Suite 3600
Seattle, WA 98101-4109
(206) 386-7598
karin.jones@stoel.com
Cooperating Attorney for ACLU-WA Foundation

Counsel for Amici Curiae

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Rules

Constitutional Provisions

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 Washington is a state affiliate 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] Defendant–Appellant consents to the filing of this amicus brief. Plaintiff–Appellee United States does not oppose the filing of an amicus brief by the ACLU this case. Pursuant to Fed. R. App. P. 29(a)(3), counsel for *amici curiae* have therefore submitted a motion for leave to file this 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 potential risks to third parties. Left unchecked by courts like this one, it poses a serious danger to both the Constitution and the broader security of the Internet.

Yet, in applying for this novel and wide-reaching warrant to install malware on multiple computers around the globe, the government failed to disclose material facts to the magistrate judge. The failure to disclose important information to the magistrate was all the more critical because confusing technological terms and processes were involved, creating a greater risk that the magistrate would misunderstand the scope of what she was being asked to authorize. Moreover, the government's failure to disclose material information interfered with the magistrate's ability to neutrally and independently evaluate the warrant application before it, as the Fourth Amendment requires. In particular, the government failed to disclose that (1) the government would use malicious software to force visitors'

computers to malfunction and install software to search their computers; (2) the malware would be installed on thousands of machines around the globe, in excess of the magistrate's authority under Federal Rule of Criminal Procedure 41; and (3) the government would operate a child pornography distribution hub. These omissions impaired the magistrate's ability to perform her duty of independent evaluation of compliance with the Fourth Amendment and to ensure that the government took necessary steps to safeguard innocent third parties who could potentially be adversely affected by this powerful tool. 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." Def.'s Br. 10–13. This section sets forth the critical background omitted in the government's warrant application.

I. Tor

Playpen was only available on 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"[2] by protecting a user's IP address,[3] location, and usage from hacking or disclosure. Using Tor is relatively easy, and millions of people do so. *See* ER.II 210. To use Tor, individuals need only download a special web browser based on the popular Firefox browser.[4]

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.

---

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

[3] 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. 19, 2017).

[4] *What is Tor Browser*?, Tor Project, https://www.torproject.org/projects/torbrowser.html.en (last visited Oct. 19, 2017).

The U.S. government originally created Tor, which serves as an essential tool for activism and free speech across the world. Journalists, bloggers, whistleblowers, human rights workers, and other activists have relied on the Tor network to avoid surveillance by potentially repressive regimes.[5]

II. Playpen

The government became interested in Playpen upon learning that unknown individuals were using the website to distribute and obtain illegal images of child pornography. On February 19, 2015, the government took control of the site and proceeded to operate it for 15 days. Def.'s Br 12. Over that time, the FBI not only maintained Playpen, but made it easier, faster, and more stable to use. ER-S.V 935 at ¶ 11, 1030 at ¶ 15; ER.I 43 (misconduct finding (3)), ER.III 527–28; ER.IV 656–78.

During the time of the government's control, the site's popularity increased—with the average number of unique weekly visitors growing from 11,000 to approximately 50,000—and images of children that had not previously been online appeared on the site. ER-S.V 935 at ¶ 11, 1030 at ¶ 15; ER.I 40–41.

[5] Users of Tor, Tor Project, https://www.torproject.org/about/torusers.html.en (last visited Oct. 19, 2017).

III. The Government's Malware

Because Playpen was only available through Tor, which masked the Internet Protocol (IP) address of Playpen users, the FBI decided to use malware to force the visitors' computers to disclose their IP address and other identifying information once it began operating the site.

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.[6] Instead of using the term malware in applying for the warrant here, the government used a sterilized term—"Network Investigative Tool," or "NIT"—a term not generally used in computer science.

In this case, the government's malware consisted of two important pieces: a "payload," computer code that instructed each computer that visited Playpen to send identifying information back to the government, and an "exploit," 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

[6] Malware, Dictionary.com, http://www.dictionary.com/browse/malware (last visited Oct. 19, 2017). The term is formally defined by the U.S. National Institute of Standards and Technology 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 Publication (2013), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

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 visitor's browser. 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.[7]

The potential for harm and intrusiveness posed by the exploit 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 in *United States v. Michaud*, U.S. District Court for the Western District of Washington No. 15-CR-05351-RJB at 9-10 (the exploit "allows a third party to tell 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 that a "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.* 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

[7] DKt no 58-1 para 4, declaration of government expert Professor Brian N. Levine.

security of the several hundred million users of Firefox. Mozilla Press Center, *Mozilla at a Glance*, https://blog.mozilla.org/press/ataglance; *see also* Mozilla's Motion To Intervene at 2, 3, 1.

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 manner of the search's execution. *See United States v. Hillyard*, 677 F.2d 1336, 1339 (9th Cir. 1982). The Fourth Amendment generally requires that, before conducting a search, the government must submit a warrant application to a neutral and detached judge. That judge is "charged with upholding" the "safeguards of the Fourth Amendment" by independently evaluating the application. *United States v. Rettig*, 589 F.2d 418, 422 (9th Cir. 1978). This judicial review requirement is "[t]he bulwark of the Fourth Amendment," *Franks v. Delaware*, 438 U.S. 154, 164 (1978), and 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).

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;'" rather, the government must present her with sufficient information to "make an independent evaluation of the matter." *Id.* (quoting *Illinois v. Gates*, 462 U.S. 213, 239 (1983)); *see also United States v. Comprehensive Drug Testing, Inc.* (*CDT*), 621 F.3d 1162, 1178 (9th Cir. 2010) (en banc) (Kozinski, J., concurring) (recognizing that the government has a "duty of candor in presenting a warrant application" and noting that "[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.").

The government's duty to disclose extends to all facts necessary for the judge to evaluate the warrant's reasonableness, including probable cause, *Franks*, 438 U.S. at 164; *Gates*, 462 U.S. at 239; particularity, *Hillyard*, 677 F.2d at 1339; *Rettig*, 589 F.2d at 422–23; and the manner of the search's execution. *See*

VonderAhe v. Howland, 508 F.2d 364, 370 (9th Cir. 1974); *Berger v. New York*, 388 U.S. 41, 57 (1967) (requiring that "precise and discriminate procedures" are in place (quotation marks omitted)). Moreover, magistrates must consider whether proposed searches pose indiscriminate risks to third parties or are unduly excessive in their means. *See, e.g.*, *Langford v. Superior Ct. of L.A. Cty.*, 43 Cal.3d 21, 233 Cal.Rptr. 387, 729 P.2d 822, 827 (Cal. 1987) (holding that, because a motorized battering ram can cause "potential danger from collapse of building walls and ceilings or through rupture of utility lines," which could cause fires that "could threaten the safety not only of occupants, but of entire neighborhoods," "routine deployment of the ram to enter dwellings must be considered presumptively unreasonable unless authorized in advance by a neutral magistrate, and unless exigent circumstances develop at the time of entry"); *Bing ex rel. Bing v. City of Whitehall*, 456 F.3d 555, 570 (6th Cir. 2006) (unreasonable under the Fourth Amendment to "employ a flashbang device [to enter a house] with full knowledge that it will 'likely' ignite accelerants and cause a fire"); *Boyd v. Benton Cty.*, 374 F.3d 773, 779 (9th Cir. 2004) ("[G]iven the inherently dangerous nature of the flash-bang device, it cannot be a reasonable use of force under the Fourth Amendment to throw it 'blind' into a room occupied by innocent bystanders absent a strong government interest, careful consideration of alternatives and appropriate measures to reduce the risk of injury.").

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 owed by the affiant to the magistrate and its critical connection to the magistrate's independent evaluation of the warrant's compliance with the Fourth Amendment. *See* 850 F.3d. at 1116–19. The Court held that "[b]y providing an incomplete and misleading recitation of the facts and withholding [certain] images," the government prevented the 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. As this Court has recognized,

computer searches like the one at issue here raise unique challenges to keeping a search 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 1179 (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 . . . ."); *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) ("Because it is common practice for people to store innocent and deeply personal information on their personal computers, a digital search of [electronically stored information] will also frequently involve searching personal information relating to the subject of the search as well as third parties.").

In such contexts, society "must rely on the good sense and vigilance of our magistrate judges, who are in the front line of preserving the constitutional

freedoms of our citizens while assisting the government in its legitimate efforts to prosecute criminal activity." *CDT*, 621 F.3d at 1179. But judges can only fulfill that role if law enforcement fully and candidly discloses all relevant facts in the search warrant application—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. As Defendant–Appellant in part sets forth, *see* Def. Br. 54–66, the government omitted or misrepresented several categories of facts, consisting of information the government possessed but chose not to disclose to the magistrate. The government could have told the magistrate how a more targeted search of specific suspects was possible, but did not. It could have disclosed the risk that the malware would result in overbroad searches, and the facts about damage the malware could do to people's computers, but it did not. And it failed to fully set forth the potential of the search to put at risk both third parties—including innocent Tor and Firefox users—and the security of the entire Internet more generally. Finally, it failed to disclose the global reach of the warrant. 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," rendering the warrant unconstitutional.

A. The Government Failed to Disclose That It Had the Information Necessary to Execute a Narrower, More Targeted Search of Specific Suspects.

When applying for the search warrant to authorize the government's use of malware, the government had particularized information about Playpen users due to the government's control of the server, but failed to offer it to the magistrate. As Defendant–Appellant explains, the government possessed the user names of 158,000 "members" of the Playpen site and detailed data about their activities on the site, such as the specific pictures or videos they viewed. *See United States v. Tippens*, Case No. 17-30117, Defendant–Appellant's Opening Brief, Dkt No. 6, p. 59 (citing ER-S.V 939-941, 1032-33). The FBI also had IP addresses for approximately 1,000 users before the NIT searches. *See id.* But rather than ask the magistrate for a warrant that would target the malware at specific members, using the information at its disposal as a result of its seizure of the site, the government took an impermissible bulk approach and instead sought a warrant that sought to infect *any* visitor to the site.

The warrant application failed to note the government's alternative option for identifying specific visitors to the Playpen site based on particularized facts regarding their activities on the site. Because the government operated the server

that hosted the Playpen site, it would be able to view and create records of (log) users' specific activities. Therefore, it could track, as to each user, the specific information posted or accessed by that user and the frequency with which the user engaged in such activities. Using that specific, individualized information, the government could have sought warrants based on particularized facts, linked to individual users and their known activities on the site. But the government chose not to take that approach, even though it had the capability to do so. *See United States v. Knowles*, 207 F. Supp. 3d 585, 593 (D.S.C. 2016) ("[I]n practice the FBI configured the NIT to activate only when a user accessed certain posts within Playpen. The NIT did not activate when a user reached Playpen's home page, created an account, or logged into that account.").

Instead, the government used the NIT to infect and search over 8,000 computers. The warrant application broadly sought to deploy the NIT 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-S.V. 947 at ¶ 36 (emphases added); *see also id.* at 945, ¶ 32. The government violated the Fourth Amendment by failing to adhere to the "duty of candor" necessary to enable the magistrate to independently evaluate particularity and the

manner of executing the warrant. *Hillyard*, 677 F.2d at 1339; *Perkins*, 850 F.3d 1109, 1116; *CDT*, 621 F.3d at 1178.

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

As noted above, this Court has recognized the particular intrusiveness of computer searches and urged caution in issuing warrants targeting computers due to the risk of "over-seizing" of evidence. *CDT*, *supra*. The government's failure here to disclose the existence and operation of an important piece of the malware it used – 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 it did not mention the other piece – the "exploit" (i.e., how it would do so). This misled the magistrate about the scope of the computer search's intrusiveness.

Exploit code can give government agents expansive access to the user's computer. Depending on how the payload code operates, the government could access files on the machine, searching stored documents, photos, or more. An exploit like the one used in this case could also log a user's keystrokes, enabling the government to obtain passwords, read emails, and track browsing history. 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 magistrate's independent

oversight of the operation of the government's malware is a critical check because of the significant potential for an overbroad search that accesses this kind of data.

In computer searches where the government has access to private data intermingled with data for which there is probable cause, the magistrate has an important role to play in policing the government's conduct both before and after the search. *See CDT*, 621 F.3d at 1178 (Kozinski, J., concurring). The magistrate is charged with ensuring that investigator access to intermingled data on computers does not run afoul of the Fourth Amendment. But here, the magistrate was not told that the government was using an exploit at all. Instead, the 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.

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 CDT*, 621 F.3d at 1178 (Kozinski, J., concurring). For example, the government should "forswear reliance on the plain view doctrine or any similar doctrine that would allow it to retain data to which it has gained access only

because it was required to segregate seizable from non-seizable data," *id.*, ensuring that the purpose of the NIT as described in the affidavit remains linked to any proffered probable cause. Likewise, the government should describe how it intends to sort, separate, and dispose of non-responsive data. *See id.* at 1179; *see also id.* ("To that end, the warrant application should normally include, or the issuing judicial officer should insert, a protocol for preventing agents involved in the investigation from examining or retaining any data other than that for which probable cause is shown."); *id.* ("Once the data has been segregated (and, if necessary, redacted), the government agents involved in the investigation should be allowed to examine only the information covered by the terms of the warrant."). By failing to address the full capabilities of the NIT in this case or NITs more generally, the government's affidavit presented the magistrate with only a partial view of what was at stake.

Had the magistrate judge had reason to know that this kind of vigilance might be required, she might have considered imposing 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 designed to uncover only the information for which the government had probable cause, and/or implemented protocols requiring the government to destroy non-responsive data or data that it would not use in a criminal investigation. Because the magistrate judge could not have understood the full scope of what the malware discussed in the warrant was going to do when the government failed to fully explain, she could not effectively assess whether the government was doing enough to minimize searches of innocent users' computers or to limit the data that the NIT collected on the target machines. The magistrate's duty to independently evaluate the warrant application was necessarily impaired. *Perkins*, 850 F.3d 1109, 1116; *CDT*, 621 F.3d at 1178.

C. The Government Failed to Disclose That It Intended to Execute the Warrant in a Way That Created Security Risks To Innocent, Non-Targeted Users.

The government's use of exploit code posed risks that the search would violate the Fourth Amendment by infecting innocent users, but the government's failure to disclose those risks prevented the magistrate from considering the propriety of relevant protections aimed at mitigating those harms. The need to include such protections in electronic surveillance orders is well established. *See, e.g.*, *Berger*, 388 U.S. at 59–60 (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 whose records are intermingled with the suspects'); *Ricks v. State*, 537 A.2d 612, 621 (Md. 1988) (describing minimization procedures applied to video surveillance, including when, where, and for how long police can operate the camera, in order to protect "communications and activities not otherwise subject to the order"); *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"); 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 relating to whether it can retain exclusive control of the tool, either before or after deploying it. For example, the government may lose control of malware if an insider leaks or sells the tools or if the government itself is hacked. 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.

The risk that the government will lose control of exploits is not theoretical. In 2016, the public learned that an entity calling itself the Shadow Brokers obtained National Security Agency ("NSA") malware from an external NSA "staging server." Following some initial attempts to sell the exploits, the Shadow Brokers dumped dozens of NSA hacking tools online for free in April 2017.[8] And in March 2017, a leak exposed thousands of pages of Central Intelligence Agency ("CIA") records documenting some of the CIA's hacking exploits,[9] including an exploit for a critical vulnerability in common routers and switches.[10] These incidents make clear the risk of the government losing control of malware and resulting damage to innocent parties' systems.

But the government's warrant application in this case makes no reference at all to the notion that the malware it was asking permission to use could have spillover effects on individuals not targeted by the warrant. The magistrate judge was not told that the search in this case involved an undisclosed exploit affecting the Tor and Firefox browsers. If the exploit got into the wrong hands, hundreds of millions of users could have been at risk. A fully apprised magistrate could have

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

[9] 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.

[10] *See id.*

inquired into the means the government is using to keep those exploits secured from unauthorized people—inside and outside of the agency—who might use and abuse them. Once again, the magistrate's function was unconstitutionally usurped. *Perkins*, 850 F.3d at 1118.

D. The Government Failed To Make Its Plan to Operate a Child Pornography Site Clear to the Magistrate.

The magistrate's duty to evaluate the "manner of the search's execution" (*Hillyard*, *supra*) was also significantly impaired by the government's failure to divulge its role in increasing distribution of child pornography. For a period of 15 days after the warrant was issued on February 20, 2015, the government became the world's largest distributor of child pornography through its operation of Playpen. ER-S.V 935 at ¶ 11, 1030 at ¶ 15. During its tenure in that role, the government not only maintained tens of thousands of illegal images and videos on the site, but it also *actively encouraged* increased viewership by making improvements to the website to upgrade its speed, accessibility, and file-hosting features and affirmatively posting announcements about those improvements on the site. *See* ER.I 43; ER-S.V 861-62, 871-93, 941 at ¶ 24; ER.III 527-28; ER.IV 656-676.

While the government ran the site, tens of thousands of visitors posted approximately 13,000 links to images or video files of child pornography, including many images not previously circulated on the Internet, which harmed

additional children. ER.I 40-41. Over the same period, visitors clicked on 67,000 unique links to such images and videos. ER-S.V 914-15. Each time a visitor uploaded an image, posted a link, or clicked on content, the children exploited in those images were victimized anew. *See United States v. Hammond*, 2016 WL 7157762, *5 (N.D. Cal. Dec. 8, 2016) ("[T]he government itself has rightly taken the position that 'young victims are harmed every time an image is generated, every time it is distributed, and every time it is viewed.'"). The government "us[ed] the child victims as bait . . . without informing the victims and without the victims' permission – or that of their families." ER.I 43.

The warrant application obfuscated the government's plans to continue to operate the Playpen server. The government told the magistrate judge that it would move the seized Playpen website to a government-controlled computer server in Virginia and that "the TARGET WEBSITE will continue to operate from the government-controlled computer server." Affidavit at ¶ 30. The use of the passive voice here obfuscated the government's active role in, in its own words, "harm[ing]" "young victims." *See Hammond*, 2016 WL 7157762 at *5 (quoting government brief).

Moreover, the government further represented that "[s]uch a tactic is necessary in order to locate and apprehend the TARGET SUBJECTS who are engaging in the continuing sexual abuse and exploitation of children, and to locate

and *rescue children from the imminent harm of ongoing abuse and exploitation*." Affidavit at ¶ 30 (emphasis added). This would strongly suggest to the magistrate that the government planned to immediately end access to and posting of the exploitive images. In fact, the government enabled individuals to post and view nearly 70,000 images for weeks in order to prosecute fewer than 140 people.

As the District Court in this case articulated, once one knows how the search was executed, "[i]t is easy to conclude that the Government acted outrageously here." ER.I 43. The omission of this information violated the Constitution.

E. The Government Failed to Disclose the Anticipated Scope of the Warrant.

The government vastly understated the scope of the search and violated its "duty of candor" (*CDT*), as well as the then-applicable version of Federal Rule of Criminal Procedure 41, by failing to clearly inform the magistrate that, pursuant to the warrant, it would be searching thousands of computers outside the Eastern District of Virginia. The warrant and its attachments indicated that the property to be searched was located in the Eastern District of Virginia. Case No. 2:15-cr-00274-MJP, Document 48-1 Filed 03/07/16, Application for a Search Warrant (p. 3 of exhibit), Search and Seizure Warrant (p. 4); but see Affidavit stating that the affiant does not know the location of computers to be searched (Para. 29, 30). The government represented that the Playpen server it had located in the Eastern District was the "TARGET computer" and the visitors' machines were merely

"activating computers." In fact, the visitors were the targets of this warrant. It was information on the visitors' machines that the government sought to search and obtain. The government knew that Playpen visitors came from around the world, that the NIT would collect information from any computer that connected to that particular Playpen web page, and that it had not configured the NIT to only send identifying information for Eastern District of Virginia computers. But calling the malware server the TARGET and the targets "activators" helped the government claim that the search would take place in the Eastern District of Virginia. As a result, the government obtained a warrant for a search in the District that it nevertheless used to gather information from computers around the country and around the world, in violation of Rule 41. *See United States v. Levin*, 186 F. Supp. 3d 26, 36 (D. Mass. 2016).

CONCLUSION

As delineated above, the government omitted many critical facts from the warrant application. As in *Perkins*, "[b]y 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 particularity, overbreadth, intrusiveness in the execution of the search, and risks to others, was undermined such that the magistrate could not fulfill her duty of "preserving the

constitutional freedoms of our citizens." *CDT*, *supra*. Accordingly, this Court should reverse the court below.

Respectfully submitted this 20th day of October, 2017.

s/ Jennifer S. Granick (via email authorization)
Jennifer S. Granick
(Cal. Bar No. 168423)
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
jgranick@aclu.org
bkaufman@aclu.org
veidelman@aclu.org

s/ Nancy L. Talner (via email authorization)
Nancy L. Talner
(WA Bar No. 11196)
ACLU-WA Foundation
Shankar Narayan
(WA Bar No. 31577)
ACLU-WA
901 Fifth Ave., Suite 630
Seattle, WA 98164
(206) 624-2184
talner@aclu-wa.org
snarayan@aclu-wa.org

s/ Karin D. Jones
Karin D. Jones
(WA Bar No. 42406)
Stoel Rives LLP
600 University Street, Suite 3600
Seattle, WA 98101-4109
(206) 386-7598
karin.jones@stoel.com
Cooperating Attorney for ACLU-WA Foundation

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 5,896 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.

s/ Karin D. Jones

October 20, 2017

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 20th 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/ Karin D. Jones

9th Circuit Case Number(s) 17-30117

NOTE: To secure your input, you should print the filled-in form to PDF (File > Print > *PDF Printer/Creator*).

****

CERTIFICATE OF SERVICE
When All Case Participants are Registered for the Appellate CM/ECF System

I hereby certify that 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 on (date) Oct 20, 2017 .

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.

Signature (use "s/" format) s/ Karin D. Jones

****

CERTIFICATE OF SERVICE
When Not All Case Participants are Registered for the Appellate CM/ECF System

I hereby certify that 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 on (date) .

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

I further certify that some of the participants in the case are not registered CM/ECF users. I have mailed the foregoing document by First-Class Mail, postage prepaid, or have dispatched it to a third party commercial carrier for delivery within 3 calendar days to the following non-CM/ECF participants:

Signature (use "s/" format)