No. 16-1567

IN THE UNITED STATES COURT OF APPEALS

FOR THE FIRST CIRCUIT

UNITED STATES OF AMERICA,

Appellant

v.

ALEX LEVIN,

Defendant-Appellee

On Appeal from the United States District Court

for the District of Massachusetts

Brief of *Amicus Curiae* Privacy International in support of Defendant-Appellee and in support of affirmance of the decision below

---

Caroline Wilson Palow
1st Cir. No. 1178172
Scarlet Kim
1st Cir. No. 1177295

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom
+44 (0) 20 3422 4321

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, *amicus curiae* Privacy International certifies that it does not have a parent corporation and that no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES v
STATEMENT OF INTEREST 1
INTRODUCTION 2
ARGUMENT 5
I. THE DISTRICT COURT WAS CORRECT IN HOLDING THAT THE MAGISTRATE JUDGE LACKED AUTHORITY UNDER RULE 41(b)(4) TO ISSUE THE NIT WARRANT BECAUSE THE NIT IS NOT A "TRACKING DEVICE." 5
A. The government's characterization of the NIT as a "tracking device" is based on a technically misleading description of the NIT. 5
1. The NIT uses an "exploit" and a "payload." 6
2. The NIT sends an exploit to devices in bulk 8
3. The NIT deploys the exploit to compromise the security of devices. 10
4. The NIT runs a "payload" to perform actions on the compromised devices 12
B. According to a proper technical understanding of the NIT, the NIT cannot be characterized as a "tracking device" within the meaning of Rule 41(b)(4). 13
II. THE NIT WARRANT IS INVALID BECAUSE IT AUTHORIZED EXTRATERRITORIAL SEARCHES AND SEIZURES. 16
A. International law prohibits unilateral extraterritorial searches and seizures. 16
B. Rule 41 does not authorize extraterritorial searches and seizures. 18
C. The magistrate judge lacked authority to issue the NIT warrant because it authorized extraterritorial searches and seizures. 20

D. The foreign relations risks posed by unilateral extraterritorial searches and seizures further counseled against authorization of the NIT warrant. 21

CONCLUSION 26

CERTIFICATE OF COMPLIANCE 27

CERTIFICATE OF SERVICE 28

ADDENDUM

TABLE OF AUTHORITIES

Cases

Arrest Warrant of 11 April 2000 (Dem. Rep. Congo v. Belg.) 2002 I.C.J. 3 (Feb. 14) 17

SS Lotus (Fr. v. Turk.) 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7) 17

Statutes and Rules

18 U.S.C. §1030(a)(2) 24

18 U.S.C. §3117(b) 13, 15

Fed. R. Crim. P. 41 (2011) ..... *passim*

Other Authorities

Michael Abbell, *Obtaining Evidence Abroad in Criminal Cases* (2010) 21, 22

American Bar Ass'n, *International Guide to Combating Cybercrime* (2002) 17

Patricia L. Bellia, *Chasing Bits across Borders*, U. Chi. Legal F. 35 (2001) 18

Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 Nw. J. Tech. & Intell. Prop. 1 (2014) 6, 10, 12

Sam Biddle, *Can 000000 Secretly Open Your Hotel Safe?*, Gizmodo (Sept. 6, 2011), http://gizmodo.com/5837561/can-000000-secretly-open-your-hotel-safe 7

Susan W. Brenner, *Cyber-threats and the Limits of Bureaucratic Control*, 14 Minn. J.L. Sci. & Tech. 137 (2013) 23

Mike Brunker, *FBI agent charged with hacking*, NBC News (Aug. 15, 2002), http://www.nbcnews.com/id/3078784 24

Anthony J. Colangelo, *Constitutional Limits on Extraterritorial Jurisdiction: Terrorism and the Intersection of National and International Law*, 48 Harv. Int'l L.J. 121 (2007) 22

Computer Crime & Intellectual Prop. Section, Dep't of Justice, *Prosecuting Computer Crimes Manual* (2010) 24

Computer Crime & Intellectual Prop. Section, Dep't of Justice, *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (2009) 22

James Crawford, *Brownlie's Principles of Public International Law* (8th ed. 2012) 18

Robert Cryer et al., *An Introduction to International Criminal Law and Procedure* 44 (2d ed. 2010) 17

Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale L.J. 326 (2015) 18, 19

Dep't of Justice, U.S. Attorney's Manual, Criminal Resources Manual 22, 24

Dep't of State, Foreign Affairs Manual 21

Charles Doyle, Cong. Research Serv., *Extraterritorial Application of American Criminal Law* (2016) 21

T. Markus Funk, Fed. Judicial Ctr., *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges* (2014) 21

Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, U.C. Hastings Legal Res. Paper No. 170 (2016) 23

Susan Hennessey & Nicholas Weaver, *A Judicial Framework for Evaluating Network Investigative Techniques*, Lawfare (July 28, 2016), https://www.lawfareblog.com/judicial-framework-evaluating-network-investigative-techniques 6, 7

Int'l Bar Ass'n, *Report of the Task Force on Extraterritorial Jurisdiction* (2009) 17, 22

The Jargon File (Oct. 1 2004), http://www.catb.org/jargon/index.html 7

Brian Krebs, *Espionage Hackers Target 'Watering Hole' Sites*, Krebs on Security (Sept. 25, 2012), https://krebsonsecurity.com/2012/09/espionage-hackers-target-watering-hole-sites/ 10

Zach Lerner, *A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure*, 18 Yale J.L. & Tech. 26 (2016)..... 9

Letter from Mythili Raman, Acting Assistant Att'y Gen., Criminal Div., Dep't of Justice, to Reena Raggi, Chair, Advisory Comm. on the Criminal Rules (Sept. 18, 2013) 19, 20

Terminology, Malware Attribute Enumeration and Characterization, MITRE (Jan. 2, 2014), http://maec.mitre.org/about/terminology.html 8

The New Hacker's Dictionary (Eric S. Raymond ed., MIT Press, 1996) (1983) ... 8

Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, Wired, Aug. 5, 2014, https://www.wired.com/2014/08/operation_torpedo/..... 7

Restatement (Third) of Foreign Relations Law in the United States (Am. Law Inst. 1987)..... 16, 17, 18

See Tor: Overview, Tor, https://www.torproject.org/about/overview.html.en (last visited Feb. 3, 2017) 10

Tor: Hidden Service Protocol, Tor, https://www.torproject.org/docs/hidden-services.html.en (last visited Feb. 3, 2017) 11

Tor Metrics, Tor, https://metrics.torproject.org/userstats-relay-table.html?start=2015-02-01&end=2015-02-28 (last visited Feb. 3, 2017) 20

What is Tor Browser?, Tor, https://www.torproject.org/projects/torbrowser.html.en (last visited Feb. 3, 2017) 10

Matthew C. Waxman, *Self Defense Force Against Cyber Attacks*, 89 Int'l L. Stud. 109 (2013)..... 23

STATEMENT OF INTEREST

Privacy International is a nonprofit, non-governmental organization based in London, the United Kingdom ("UK"), which defends the right to privacy around the world. Established in 1990, Privacy International undertakes research and investigations into government and corporate surveillance with a focus on the technologies that enable these practices. It has litigated or intervened in cases implicating the right to privacy in the courts of the United States, the UK, and Europe, including the European Court of Human Rights. To ensure universal respect for the right to privacy, Privacy International advocates for strong national, regional and international laws that protect this right. It also strengthens the capacity of partner organizations in developing countries to identify and defend against threats to privacy.

Privacy International files this brief with the consent of all parties.[1]

[1] Pursuant to Federal Rule of Appellate Procedure 29(a)(4)(E), counsel for *amicus curiae* state that no counsel for a party authored this brief in whole or in part, and no person other than *amicus curiae* or its counsel made a monetary contribution to its preparation or submission.

INTRODUCTION

The "network investigative technique" ("NIT") used by the government in this case is a novel, sophisticated and awesome power. Its novelty and sophistication make it difficult to grasp its operation. Yet, without this understanding, those tasked with authorizing and overseeing the NIT fail to comprehend the profoundly intrusive effect it can have on our electronic devices, upon which we increasingly depend to communicate with others, express our personal and political views, and store our most sensitive information. They may further fail to recognize the NIT's capability to affect connected devices anywhere in the world.

It seems the government would prefer to keep us in the dark. It uses vague and imprecise language, divorced from well-established technical vocabulary and concepts, to describe the NIT. By painting a picture of the NIT with such unintelligible brushstrokes, the government seeks to render a hazy impression of a tracking device. It asks us to imagine the NIT as a transmitter, like that we might affix to a vehicle, transposed to the digital realm. But the NIT is not a tracking device and therefore could not be authorized, as the government submits, pursuant to Federal Rule of Criminal Procedure 41(b)(4).

The NIT comprises distinct and intricate technical processes and components. Together, these processes and components operate to compromise the

security of the devices of untold numbers of unknown individuals. They then perform a series of actions on the devices, including locating particular categories of information and then copying and sending that information from the devices to the government. Examined separately or as a whole, none of these processes or components constitute a tracking device within the meaning of Rule 41(b)(4).

From its warrant application to its brief before this Court, the government has also downplayed the international ramifications of using the NIT. We now know that the NIT infiltrated over 8,700 devices. Over 83% of these devices were located outside of the U.S., in 120 countries and territories. This outcome was entirely foreseeable to the government at the time of its warrant application.

The NIT warrant therefore authorized the government to undertake extraterritorial action. Well-established international law prohibits the government from undertaking law enforcement functions in other countries, without those countries' consent, which the government did not seek here. This principle is reflected in the warrant authority, which does not permit judges to authorize extraterritorial action. These legal constraints protect against the foreign relations risks incurred when the U.S. acts extraterritorially, risks that are particularly amplified when the U.S. interferes with the devices of thousands of individuals abroad.

Where the government seeks to use new and complex technology to facilitate searches and seizures, that technology may not fit appropriately into existing categories of authorization. Incongruity should give the courts pause, for such technology may have unforeseen and powerful consequences, as revealed by a close and clear-eyed examination of the NIT. Here, the NIT failed to qualify as a tracking device or otherwise operate in a manner that would support the issuance of the NIT warrant. Its extraterritorial reach further renders the warrant invalid. For these reasons, this Court should uphold the decision below.

ARGUMENT

I. THE DISTRICT COURT WAS CORRECT IN HOLDING THAT THE MAGISTRATE JUDGE LACKED AUTHORITY UNDER RULE 41(b)(4) TO ISSUE THE NIT WARRANT BECAUSE THE NIT IS NOT A "TRACKING DEVICE."

The government submits that Federal Rule of Criminal Procedure 41(b)(4) authorized the magistrate judge to issue the NIT warrant. Gov't Br. 23-32. Privacy International disagrees. According to a proper technical understanding of the NIT, the NIT cannot be characterized as a tracking device within the meaning of Rule 41(b)(4).

A. The government's characterization of the NIT as a "tracking device" is based on a technically misleading description of the NIT.

The government's description of the NIT obscures how the NIT works in practice. The NIT comprises multiple distinct processes, involving the use of distinct technical components. These processes render the NIT a technique to:[2]

[2] Privacy International relies primarily on expert declarations and testimony in other criminal proceedings arising out of the government's execution of the NIT warrant to describe the NIT. These statements were elicited in conjunction with motions to compel discovery regarding the NIT pursuant to Federal Rule of Criminal Procedure 16(d). *See, e.g.*, *United States v. Matish*, No. 16-cr-16 (E.D. Va.); *United States v. Michaud*, No. 15-cr-5351 (W.D. Wa.); *United States v. Tippens*, No. 16-cr-5110 (W.D. Wa.). They currently constitute the most detailed technical information in the public domain about how the NIT operates. We rely on representations from experts for both the government, *see* Decl. of Brian Levine, *Tippens* (Sept. 22, 2016), ECF No. 58-1 (PI.Add:23); Decl. of Special Agent Daniel Alfin, *Matish* (June 1, 2016), ECF No. 74-1 (PI.Add:4), and various defendants, *see* Decl. of Christopher Soghoian, *Matish* (June 10, 2016), ECF No. 83-1 (PI.Add:1); Decl. of Matthew Miller, *Michaud* (May 9, 2016), ECF No. 191-1 (PI.Add:16), and note where these representations diverge from each other. The government's

(1) send an "exploit" to devices in bulk;

(2) deploy the "exploit" to compromise the security of those devices; and

(3) run a "payload" to perform actions on the devices.[3]

Below, we unpack and explain each of these processes and components.

1. The NIT uses an "exploit" and a "payload."

An "exploit" takes advantage of a security "vulnerability" – *i.e.* weakness or flaw – in a computer system or application.[4] *See* Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 Nw. J. Tech. & Intell. Prop. 1, 22-23 (2014) ("A vulnerability is a weakness in a system

addendum is cited as "G.Add," the supplemental appendix is cited as "SA" and Privacy International's addendum is cited as "PI.Add."

[3] Privacy International does not address aspects of the NIT that do not directly pertain to whether it can be properly characterized as a tracking device. These aspects include its generation of a "unique identifier" to distinguish information collected from different devices and a "server component," which refers to the FBI system for receiving, recording and storing information transmitted from devices. *See* Alfin Decl. ¶¶18-19, 24-25 (PI.Add:7-8).

[4] Experts for the government do not dispute that it used an exploit, but have not taken a clear position on whether the exploit constitutes part of the NIT itself. *Compare* Levine Decl. ¶4 (PI.Add:24) ("[M]y understanding of the overall process used by the FBI is as follows. A defendant's computer connected using the Tor network to the Playpen website . . . . Retrieving certain pages from the Playpen website resulted in the download of the FBI's exploit and payload programs.") *with* Alfin Decl. ¶11 (PI.Add:6) ("[A]n 'exploit' allowed the FBI to deliver a set of instructions – the NIT – to Matish's computer. . . . The NIT instructions and results have been provided to the defense for review; the 'exploit' has not."). Experts for defendants in NIT cases as well as scholars following this wave of litigation agree that the exploit constitutes a component of the NIT. *See, e.g.*, Miller Decl. ¶¶2-3 (PI.Add:16-17) (agreeing with another expert that there are "four major components" to the NIT and proceeding to discuss the "exploit" as one of those components); Susan Hennessey & Nicholas Weaver, *A Judicial Framework for Evaluating Network Investigative Techniques*, Lawfare (July 28, 2016), https://www.lawfareblog.com/judicial-framework-evaluating-network-investigative-techniques (describing the "exploit" as one of "a number of distinct components" comprising the NIT).

that can potentially be manipulated by an unauthorized entity to allow exposure of some aspect of the system."). A physical world analogy to an exploit might be a trick to unlock a hotel safe unbeknownst to the user, such as by entering an override code. *See, e.g.*, Sam Biddle, *Can 000000 Secretly Open Your Hotel Safe?*, Gizmodo (Sept. 6, 2011), http://gizmodo.com/5837561/can-000000-secretly-open-your-hotel-safe.

An exploit, by taking advantage of a security vulnerability in a computer system or application, permits a "payload" to run. *See* Hennessey & Weaver, *supra* ("[T]he exploit opens a window in the owner's house that the owner believed was locked but which can be removed from the frame . . . and lets in the payload . . ."). Payloads are sometimes characterized as "malware," a term that may be more familiar to the Court.[5] Malware, a contraction of "malicious software," refers to computer code designed to perform actions on a system that, but for the malware, would not occur. *See* The Jargon File (Oct. 1, 2004),

[5] Experts for the government do not dispute that it used a payload. *See, e.g.* Levine Decl. ¶4 (PI.Add:24); Alfin Decl. ¶7 (PI.Add:5). The government has however, in certain circumstances, objected to the use of the term "malware" to describe any part of the NIT. *See, e.g.*, Gov't's Surreply to Defendant's Motion to Compel Discovery at 11-13, *Matish* (June 1, 2016), ECF No. 74. Nevertheless, computer security experts have used this term to describe the NIT. *See* Soghoian Decl. ¶¶5-12 (PI.Add:2-3); Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, Wired (Aug. 5, 2014) https://www.wired.com/2014/08/operation_torpedo/ ("From the perspective of experts in computer security and privacy, the NIT is malware, pure and simple.") (describing prior FBI operations employing NITs).

http://www.catb.org/jargon/index.html (entry for "malware").[6] A "payload," in the computer security context, can refer to that part of malware that actually performs those actions. *See Terminology*, Malware Attribute Enumeration and Characterization, MITRE (Jan. 2, 2014), http://maec.mitre.org/about/terminology.html ("[A] malware's payload . . . is directly tied into the purpose behind the malware."). Extending the hotel safe analogy above, the exploit could be a method for unlocking the safe, while the payload could be any action taken once the safe is unlocked, including copying or stealing its contents.

2. The NIT sends an exploit to devices in bulk.

The first step of the NIT is to send an exploit to all devices visiting the Playpen website. *See* NIT Aff. ¶32 (G.Add:68). As the government's warrant application explains, "[i]n the normal course of operations, websites send content to visitors" and "[a] user's computer downloads that content and uses it to display web pages . . . ." *Id.* ¶33 (G.Add:68). The FBI modified the code on the Playpen site itself so that when visitors requested content from the site, that content was "augment[ed] . . . with additional computer instructions." *Id.*; Motions Hearing Tr. at 76-77, *Michaud* (Jan. 22, 2016), ECF No. 203 (PI.Add:11-12) (Alfin test.) ("We

[6] The Jargon File is a glossary of computer programming terms, originally compiled by early computer programming communities, which has also been published as *The New Hacker's Dictionary* (Eric S. Raymond ed., MIT Press, 1996) (1983).

configured the NIT to supplement the information being downloaded by the user with the NIT instructions."); *see also id*. at 112 (PI.Add:13) (Soghoian test.) ("[A] regular person just clicking around is not going to know there has been this new special code added to the web site."). What the government vaguely describes as "additional computer instructions," NIT Aff. ¶33 (G.Add:68); Gov't Br. 27, is, as clarified by one of its own experts, instructions to send an exploit. Levine Decl. ¶4 (PI.Add:24) ("Retrieving certain pages from the Playpen website resulted in the download of the FBI's exploit . . . .").

This mode of delivery was bulk by nature, as every visitor to the targeted website would receive the exploit. The warrant application observed that, according to historical data about the Playpen site, it received over 1,500 unique users daily and over 11,000 unique users weekly. NIT Aff. ¶19 (G.Add:62). The application requested "authority to use the NIT, which will be deployed on the TARGET WEBSITE . . . to investigate any user or administrator who logs into the TARGET WEBSITE." *Id*. ¶32 (G.Add:68). The bulk nature of this technique is why it is commonly known as a "watering hole attack." *See* Zach Lerner, *A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure*, 18 Yale J.L. & Tech. 26, 41-42 (2016) (describing the FBI's use of watering hole attacks). Such attacks are designed to target unknown individuals in a group, by identifying websites (*i.e.*, watering

holes) that their members frequent and installing code on those sites, which transmit an exploit to visiting devices.[7]

3. The NIT deploys the exploit to compromise the security of devices.

Once the exploit has been sent to a device, it takes advantage of a vulnerability in the Tor Browser program.[8] *See* Motions Hearing Tr. 114 ("[T]he NIT . . . bypassed the security controls within the Tor browser . . . ."); *see also* Mozilla Motion 4 ("[T]he Exploit took advantage of a vulnerability in the browser software used by the Defendant."). The Tor Browser consists of a modified version of Mozilla's Firefox browser and Tor software. *What is Tor Browser?*, Tor, https://www.torproject.org/projects/torbrowser.html.en (last visited Feb. 3, 2017). Through the Tor Browser, users can connect to the Tor network, which protects their anonymity while using the internet. *See Tor: Overview*, Tor,

---

[7] The term "watering hole attack" is commonly used in the computer security field, even though the government has objected to its use to describe any part of the NIT. *See* Soghoian Decl. ¶10 n.9 (PI.Add:3) ("The D[OJ] has taken the position that bulk delivery of NITs in operations like Playpen are not watering hole attacks. . . . [T]he D[OJ] and the technical community do not see eye to eye."); *see also* Brian Krebs, *Espionage Hackers Target 'Watering Hole' Sites*, Krebs on Security (Sept. 25, 2012), https://krebsonsecurity.com/2012/09/espionage-hackers-target-watering-hole-sites/ (describing watering hole attacks).

[8] The government has not denied that the exploit takes advantage of a vulnerability in the Tor Browser program but has not disclosed the exploit itself. Accordingly, the exact nature of the exploit remains unclear, which may account for why it has been described as both code and command. *Compare* Alfin Decl. ¶11 (PI.Add:6) ("As used here, a computer 'exploit' consists of lines of code that are able to take advantage of a software vulnerability.") *with* Mozilla's Motion to Intervene or Appear as *Amicus Curiae* at 4, *Michaud* (May 11, 2016), ECF No. 195 ("[T]he exploit is not malware or a program, but a command . . . ."); *see generally* Bellovin et al., *supra*, at 23 (explaining that an exploit "can be a software program, or a set of commands or actions").

https://www.torproject.org/about/overview.html.en (last visited Feb. 3, 2017). The Tor network also makes it possible for individuals to host websites, known as "hidden services," without revealing the location of the site. *See Tor: Hidden Service Protocol*, Tor, https://www.torproject.org/docs/hidden-services.html.en (last visited Feb. 3, 2017). A user can only visit a "hidden service" by using the Tor network; Playpen was one such hidden service.

In narrow terms, the exploit operated to circumvent the security protections of the Tor Browser, which normally prevents websites from determining certain identifying information of visitors. More broadly, however, by circumventing the security protections of the Tor Browser, the exploit compromised the security of the devices themselves.[9] *See* Motions Hearing Tr. 115-16 (PI.Add:14-15) ("Q. [T]he NIT bypasses security or overrides security features on the [target] computer. . . . A. That sounds right."); Miller Decl. ¶2 (PI.Add:16) ("[T]he NIT . . . compromised the security settings on [the defendant's] computer . . . ."); Mozilla Motion 3 ("Mozilla has reason to believe that the Exploit . . . is an active

[9] Experts for the government do not dispute that the exploit compromised the security of devices, but dispute that the exploit made "*fundamental* changes or alterations to a computer system or to disable its security firewall" (while admitting that these scenarios are "theoretically possible"). Alfin Decl. ¶¶11, 14 (PI.Add:6) (emphasis added); Levine Decl. ¶6(b) (PI.Add:25) (stating "there is no evidence to support" the hypothesis that "an FBI exploit or payload made *permanent* changes to the security settings or any other settings of the defendants' computers") (emphasis added).

vulnerability in its Firefox code base that could be used to compromise users and systems running the browser.").

4. The NIT runs a "payload" to perform actions on the compromised devices.

Once the exploit has compromised the security of a device, the NIT runs a payload.[10] *See* Levine Decl. ¶4 (PI.Add:24) ("Much like a tool to open a locked door to a house, the purpose of the exploit was to allow for the execution of the payload program on a defendant's computer."). Here, the payload was designed in part to locate certain information on the device to assist "in identifying the user's computer, its location, and the user of the computer." NIT Aff. ¶34 (G.Add:68-69) (listing the information sought by the government); Levine Decl. ¶4 (PI.Add:24) ("The payload program queried a defendant's computers for certain information . . . ."). The payload was further designed to copy and transmit that information from the device to the government.[11] *See* Alfin Decl. ¶11 (PI.Add:6) (describing the NIT

[10] In part because the exact nature of the exploit remains unclear, *see supra* note 8, the details of how the payload was delivered to devices are also murky. A "dropper" is a component of malware that typically "installs the payload on the target system." Bellovin et. al, *supra*, at 24. However, a dropper can be "single stage, a program that executes . . . as a direct result of a successful exploit," which "carries a hidden instance of the payload," or "it can be multi-stage, executing on the target system, but downloading . . . the payload . . . from a remote server." *Id*.

[11] The "actual IP address," one of the categories of information sought by the government was not technically seized from the devices themselves. Rather, it appears that as the data copied from the devices was transmitted to the government, the actual IP address attached itself to that data and was thereby revealed to the government. The technical details of this aspect of the NIT are beyond the scope of this brief.

as having "gathered specific information . . . and transmitted that information to government controlled computers").

B. According to a proper technical understanding of the NIT, the NIT cannot be characterized as a "tracking device" within the meaning of Rule 41(b)(4).

The definition of "tracking device," as used in Rule 41, is "an electronic or mechanical device which permits the tracking of the movement of a person or object." 18 U.S.C. §3117(b); Fed. R. Crim. P. 41(a)(2)(e) (incorporating this definition). The government explains that, "applied to older technologies, the Rule contemplates that a tracking device may be a mechanical tool used to track the movement of a tangible object," such as a transmitter affixed to a vehicle. Gov't Br. 27. Translated to "newer technologies," the government submits that "the Rule envisions that a tracking device may be an electronic device used to track the movement of information – *e.g.*, computer instructions embedded in digital content traveling on data highways, like the NIT in this case." *Id*.

The NIT is not a single "electronic device" or even a single "set of 'computer instructions.'" The very first step of the NIT reveals it comprises multiple sets of "computer instructions": the "instructions" on the modified Playpen site to send the exploit to devices in bulk as well as the exploit and the payload themselves. Furthermore, the NIT, taken as a whole, does not operate to "track the movement of information." Rather, its primary functions are to

compromise the security of many unknown devices in bulk in order to perform a series of actions on those devices.

The tracking device analogy also collapses if we separately examine each of the processes and components that make up the NIT. The government suggests that the first step of the NIT – the watering hole attack – served a tracking function, by "follow[ing] illegal child pornography content requested by a user who accessed Playpen." Gov't Br. 28. But the watering hole attack neither follows nor tracks information. Rather, it *sends an exploit* to visitors to the Playpen website. *See* Motions Hearing Tr. 112 (PI.Add:13) ("[T]he website tells the web browser, 'Do this.' The code is downloaded to . . . the Tor browser . . . [a]nd it is only when the instructions are received by the Tor browser . . . that they are run on that computer . . . ."). And even if we were to analogize the watering hole attack to the "installation" of a tracking device, it would require contemplating installation on thousands of vehicles simultaneously, whose locations and owners are unknown.[12]

In any event, neither the exploit nor the payload can be fairly characterized as a "tracking device." The exploit operates exclusively to compromise the security of devices so as to permit the payload to run. The payload then performs a series of

[12] The government further argues that the NIT "was installed in the Eastern District of Virginia, as required by Rule 41(b)(4)." Gov't Brief 29. Because Privacy International disputes that the NIT is a tracking device, it does not address this argument. It notes, however, that the defendant-appellee's computer never physically entered or left the Eastern District of Virginia. *See* Amended Memorandum & Order 14 (G.Add:14).

actions – locating, copying, and sending information from those devices to the government. A tracking device, according to the government's own analysis, performs only the last step. Gov't Br. 27 ("Similar to a transmitter affixed to an automobile that is programmed to send location-enabling signals (like GPS coordinates) . . . , the NIT . . . was designed to send location-enabling information . . . back to a government-controlled computer . . . .").

Even to the extent that the final step of the payload – transmission of information to the government – overlaps with how a tracking device operates, critical differences remain. Unlike a tracking device, the payload does not transmit information related to the *movement* of anything. *See* 18 U.S.C. §3117(b) (defining "tracking device," as used in Rule 41, as "an electronic . . . device which permits the tracking of the *movement* of a person or object") (emphasis added). Nor is the payload even confined to transmitting information related solely to the location of devices. Rather, the payload was explicitly designed to locate, copy, and transmit multiple categories of information – such as the device's "host name" and active operating system username – beyond those that would simply assist in identifying the location of the devices. *See* NIT Aff. ¶34 (G.Add.:69).

For the reasons set forth above, the NIT cannot properly be characterized as a "tracking device" within the meaning of Rule 41(b)(4).

II. THE NIT WARRANT IS INVALID BECAUSE IT AUTHORIZED EXTRATERRITORIAL SEARCHES AND SEIZURES.

The government explains that "[t]he FBI used the NIT to identify the IP addresses of hundreds of Playpen users located across the country," but noticeably fails to mention the extraterritorial reach of its operation. Gov't Br. 8. In separate criminal proceedings arising out of the government's execution of the NIT warrant, the government recently disclosed that the NIT affected thousands of devices located in 120 countries and territories. Evidentiary Hearing Tr. at 18, *Tippens* (Nov. 1, 2016), ECF No. 103 (PI.Add:20). Specifically, the NIT returned 8,713 IP addresses, 7,281 (over 83%) of which were foreign. *Id*. at 39 (PI.Add:22).

Much of the litigation around the country challenging the validity of the NIT warrant, including in this case, has centered around the domestic jurisdictional limitations imposed by Rule 41. *See* Gov't Br. 17-19 (citing cases). But absent from this debate is a consideration of the extraterritorial jurisdictional limitations on the warrant authority. Below, Privacy International discusses the international and domestic legal bases for these limitations. Privacy International then describes some of the foreign relations implications of authorizing the NIT warrant.

A. International law prohibits unilateral extraterritorial searches and seizures.

International law subjects a state to limitations on its authority to exercise extraterritorial jurisdiction. *Restatement (Third) of Foreign Relations Law in the*

United States §401 (Am. Law Inst. 1987). A state exercises what is called enforcement jurisdiction when it undertakes some form of executive action.[13] In the criminal context, the U.S. exercises enforcement jurisdiction when its law enforcement "effect[s] legal process coercively, such as to arrest someone, or to undertake searches and seizures." Robert Cryer et al., *An Introduction to International Criminal Law and Procedure* 44 (2d ed. 2010).

Enforcement jurisdiction is generally constrained by territory. Thus, "[a] state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state . . . ." *Restatement (Third)*, *supra*, at §432(2); *see also* Int'l Bar Ass'n, *Report of the Task Force on Extraterritorial Jurisdiction* 9-10 (2009) ("[A] state cannot investigate a crime, arrest a suspect, or enforce its judgment or judicial processes in another state's territory without the latter state's permission.") (citing SS Lotus (Fr. v. Turk.) 1927 P.C.I.J. (ser. A) No. 10, at 18 (Sept. 7); Arrest Warrant of 11 April 2000 (Dem. Rep. Congo v. Belg.) 2002 I.C.J. 3 ¶¶4, 49, 54 (Feb. 14)). These restrictions apply to remote searches and seizures of devices located abroad. *See* American Bar Ass'n, *International Guide to Combating Cybercrime* 154 (2002) (criticizing

[13] A state can exercise three types of jurisdiction: (1) prescriptive ("*i.e.* to make its law applicable to the activities, relations, or status of persons, or the interests of persons in things"), (2) adjudicative ("*i.e.* to subject persons or things to the process of its courts"), or (3) enforcement ("*i.e.* to induce or compel compliance . . . with its laws or regulations"). *Restatement (Third)*, *supra*, at §401.

unilateral cross-border data searches as "inevitably allow[ing] one state to transgress upon another state's sovereignty by searching and seizing property . . . that is physically located within that second state's territory"); Patricia L. Bellia, *Chasing Bits across Borders*, U. Chi. Legal F. 35, 77-80 (2001) (explaining why "the customary international law rule against one state conducting investigative activities in another state's territory provides a strong basis for states to object to remote cross-border searches of data within their territory").

B. Rule 41 does not authorize extraterritorial searches and seizures.

The warrant authority reflects the "territorial-based limits" of enforcement jurisdiction:

> The overarching rule is that the judiciary's warrant authority is territorially limited. After all, under well-accepted principles of international law, State A can exercise law enforcement actions in State B only if State B consents. As a result, judges are presumed to lack authority to unilaterally authorize extraterritorial searches and seizures.

Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale L.J. 326, 354 (2015) (citing, *inter alia*, *Restatement (Third)*, *supra*, at §432(2); James Crawford, *Brownlie's Principles of Public International Law* 478-49 (8th ed. 2012)). Thus, Rule 41 generally limits search and seizure authorization to persons or property located within the district in which the magistrate judge sits. *See* Fed. R. Crim. P. 41(b)(1)-(2), (4). And "[e]ven in those limited situations . . . in which judges are permitted to issue warrants authorizing out-of-district searches or seizures, such

warrants are still widely understood to be subject to territorial-based limitations." Daskal, *supra*, at 355; *see also id*. (noting that the "instances [under Rule 41(b)(5)] in which magistrate judges are explicitly authorized to issue a warrant with extraterritorial reach . . . extend to locations where the United States already exerts significant (if not exclusive) regulatory authority, thereby avoiding potential conflict with foreign jurisdictions and maintaining respect for other nations' sovereign authority to enforce the law"). The government's own commentary on its proposed amendment to Rule 41 – which now permits out-of-district searches where the location of "the media or information . . . has been concealed through technological means" – observes that "[i]n light of the presumption against international extraterritorial application . . . this amendment does not purport to authorize courts to issue warrants that authorize the search of electronic storage media located in a foreign country or countries." Letter from Mythili Raman, Acting Assistant Att'y Gen., to Reena Raggi, Chair, Advisory Comm. on the Criminal Rules 2 (Sept. 18, 2013) (SA:4) ("Raman Letter"); *see also infra* note 14. The government therefore acknowledges, at least in principle, that Rule 41 does not – and did not prior to its amendment on December 1, 2016 – authorize courts to issue warrants that authorize extraterritorial searches and seizures using techniques such as the NIT.

C. The magistrate judge lacked authority to issue the NIT warrant because it authorized extraterritorial searches and seizures.

By authorizing the NIT warrant, the magistrate judge authorized the government to conduct extraterritorial searches and seizures.[14] The NIT's extraterritorial reach was foreseeable at the time the government made its warrant application. The government submitted that "using the Tor network . . . obscure[e]s a user's true location" and accordingly explained the NIT's purpose as "reveal[ing] to the government . . . information that may assist in identifying the user's computer, *its location*, and the user of the computer." NIT Aff. ¶¶8, 34 (G.Add:11, 68-69) (emphasis added); *see also supra* 11 (explaining that as a "hidden service," the Playpen website required visitors to connect to it using the Tor network). If the physical location of a device is cloaked, it may be anywhere in the world. Moreover, at the time of the government's warrant application, over 80% of Tor users were connecting to the network from outside the U.S. *Tor Metrics*, TOR, https://metrics.torproject.org/userstats-relay-table.html?start=2015-02-

[14] The government accepts that an extraterritorial search or seizure occurs if the device from which information is searched or seized is located abroad. On December 1, 2016, amendments proposed by the DOJ to Rule 41 went into effect, authorizing magistrate judges "to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if . . . the district where the media or information is located has been concealed through technological means." Fed. R. Civ. P. 41(b)(6). In a letter to the Rules Committee, the DOJ explained that "[i]n light of the presumption against international extraterritorial application . . . this amendment does not purport to authorize courts to issue warrants that authorize the search of electronic storage media located in a foreign country or countries." Raman Letter, *supra*, at 2 (SA:2). The government therefore submits that "the search of electronic storage media located" abroad constitutes an extraterritorial search.

01&end=2015-02-28 (last visited Feb. 3, 2017) (refining search of "Top-10 countries by relay users" to the month of February 2015). Accordingly, the NIT warrant is invalid because it authorized extraterritorial searches and seizures.

D. The foreign relations risks posed by unilateral extraterritorial searches and seizures further counseled against authorization of the NIT warrant.

The magistrate judge's authorization of the NIT warrant has potentially profound foreign relations implications. As discussed above, well-established principles of international law prohibit unilateral extraterritorial searches and seizures. In accordance with these principles, the U.S. traditionally relies on consent-based mechanisms for obtaining evidence located extraterritorially.[15] The principal mechanism is a Mutual Legal Assistance Treaty ("MLAT"), a bilateral agreement containing procedures for obtaining and providing assistance in criminal matters.[16] *See* T. Markus Funk, Fed. Judicial Ctr., *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges* 5 (2014). Law enforcement agencies may also participate directly in various other types of cooperative arrangements.[17]

---

[15] For an overview of the range of consent-based mechanisms, see Michael Abbell, *Obtaining Evidence Abroad in Criminal Cases* (2010).

[16] The U.S. currently has MLATs in force with over 70 countries. Charles Doyle, Cong. Research Serv., *Extraterritorial Application of American Criminal Law* 23 (2016). MLATs are negotiated by the State Department and implemented by the DOJ's Office of International Affairs. Dep't of State, 7 *Foreign Affairs Manual* §962.1.

[17] The U.S. is, for example, a member of the International Criminal Police Organization (Interpol), which enables countries to route requests for law enforcement assistance through its

Consent-based mechanisms help avoid jurisdictional – and thereby diplomatic – conflict between states.[18] *See* Int'l Bar Ass'n, *supra*, at 30. The government itself recognizes and warns its personnel against these risks. The U.S. Attorney's Criminal Resource Manual accordingly instructs:

> The other nation may regard an effort by an American investigator or prosecutor to investigate a crime or gather evidence within its borders as a violation of sovereignty. Even such seemingly innocuous acts as a telephone call, a letter, or an unauthorized visit to a witness overseas may fall within this stricture. A violation of sovereignty can generate diplomatic protests and result in denial of access to the evidence or even the arrest of the agent or Assistant United States Attorney who acts overseas. The solution is usually to invoke the aid of the foreign sovereign in obtaining the evidence.

Dep't of Justice, U.S. Attorney's Manual, *Criminal Resources Manual* §267. The DOJ's Computer Crime and Intellectual Property Section extends this precaution to the digital realm, warning: "[S]ome countries may object to attempts by U.S. law enforcement to access computers located within their borders. Although the search may seem domestic to a U.S. law enforcement officer executing the search in the United States . . . , other countries may view matters differently." Computer Crime & Intellectual Prop. Section, Dep't of Justice, *Searching and Seizing*

---

network. Abbell, *supra*, at 9 & n.47. Moreover, federal law enforcement agencies, such as the FBI, may transmit requests for investigative assistance through their liaisons or attachés stationed at embassies and consulates abroad. *Id*. at 10 & nn.50-51.

[18] Jurisdiction, in this sense, is "a proxy for state power," defining the "legal relationship" between "the state to other sovereigns." Anthony J. Colangelo, *Constitutional Limits on Extraterritorial Jurisdiction: Terrorism and the Intersection of National and International Law*, 48 Harv. Int'l L.J. 121, 126 (2007).

Computers and Obtaining Electronic Evidence in Criminal Investigations 85 (2009) (SA:41).

Here, the government unilaterally deployed the NIT, which poses particular risks. *See* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, U.C. Hastings Legal Res. Paper No. 170 24 (2016) ("A review of applicable treaties and diplomatic communications reveals that no state has consented to the United States' launch of cross-border network investigative techniques."). If the FBI were to conduct a physical search or seizure abroad, the nature of the extraterritorial action would be clear from the outset. But in the digital realm, "incidents will probably involve a publicly ambiguous set of facts" because "[m]alicious computer code or actions in cyberspace . . . are opaque to public view, technically very complex and likely to emerge piecemeal." Matthew C. Waxman, *Self Defense Force Against Cyber Attacks*, 89 Int'l L. Stud. 109, 119 (2013); *see also* Susan W. Brenner, *Cyber-threats and the Limits of Bureaucratic Control*, 14 Minn. J.L. Sci. & Tech. 137, 171 (2013) ("[W]hen our activities migrate into cyberspace, it becomes correspondingly difficult for nation-states to ascertain the nature of the threats they confront."). As a result, other states may mischaracterize the NIT and similar techniques, heightening the risk of diplomatic conflict.

In addition, as the above excerpt from the DOJ's *Criminal Resources Manual* notes, the use of the NIT may violate the domestic law of other states. *See supra* 22. Reversing the scenario, foreign deployment of a NIT-like technique against U.S. devices in order to locate, copy and transmit information would violate U.S. law. *See, e.g.*, Computer Crime & Intellectual Prop. Section, Dep't of Justice, *Prosecuting Computer Crimes Manual* 16-19 (2010) (describing intentional access to a computer without authorisation to obtain information as a violation of 18 U.S.C. §1030(a)(2), a provision of the Computer Fraud and Abuse Act). The violation of foreign laws carries with it the risk of foreign prosecution. For instance, in 2002, Russia's Federal Security Service ("FSB") filed criminal charges against an FBI agent for remotely accessing and copying data from a Russian server.[19] Brunker, *supra*; *see also United States v. Gorshkov*, No. 00-cr-550, 2001 WL 1024026 (W.D. Wash., May 23, 2001).

The government suggests that if it is not permitted to seek authorization for the NIT pursuant to Rule 41, it may have to "resort[] to warrantless searches justified by claims of exigency." Gov't Br. 25. To the extent that the government

[19] Russia's reaction can be understood as an assertion of sovereignty. *See* Mike Brunker, *FBI agent charged with hacking*, NBC News (Aug. 15, 2002), http://www.nbcnews.com/id/3078784 (citing FSB sources "describing the criminal complaint as an effort to restore traditional law enforcement borders" and quoting one such source as stating, "[i]f the Russian hackers [who were the subjects of the FBI investigation] are sentenced on the basis of information obtained by the Americans through hacking, that will imply the future ability of U.S. secret services to use illegal methods in the collection of information in Russia and other countries").

claims that its extraterritorial action requires no authorization at all, such a position violates well-established international law and practice, which condemns the unilateral exercise of extraterritorial searches and seizures. Privacy International further counsels against a conclusion that there is no role for judicial authorization to play in the context of extraterritorial searches and seizures. In an era in which more and more of our data – emails, texts, phone calls, documents and photos – seamlessly and arbitrarily travels across borders or sits abroad, we may need to fundamentally reconsider traditional doctrines of extraterritoriality as they apply to law enforcement action. This exercise requires thoughtful and careful study, well beyond the scope of this brief, as to how best to balance privacy rights, investigative efficacy and national sovereignty in the digital era. Rule 41, however, is not sufficient on its own to authorize extraterritorial searches and seizures.

CONCLUSION

For the reasons set forth above, *amicus curiae* Privacy International respectfully requests that this Court affirm the ruling below.

Dated February 10, 2017

Respectfully submitted,

/s/ Caroline Wilson Palow
Caroline Wilson Palow
1st Cir. No. 1178172
Scarlet Kim
1st Cir. No. 1177295

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom
+44 (0) 20 3422 4321
caroline@privacyinternational.org

CERTIFICATE OF COMPLIANCE WITH FED. R. APP. P. 32

1. This brief complies with the type-volume limitation of Fed. R. Ap. P. 29(a)(5) and Fed. R. App. P. 32(a)(7)(B) because it contains 6,408 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii) (*i.e.*, cover page, corporate disclosure statement, table of contents, table of authorities, certificates of counsel, signature block, and addendum). Fed. R. App. P. 32(a)(7)(B)(i) provides that "[a] principal brief is acceptable if it . . . contains no more than 13,000 words" and Fed. R. App. P. 29(a)(5) provides that "an amicus brief may be no more than one-half the maximum length authorized by these rules for a party's principal brief" (*i.e.* 6,500 words).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Times New Roman 14 point, in Microsoft Word 2016.

Dated February 10, 2017

/s/ Caroline Wilson Palow

Caroline Wilson Palow

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom
+44 (0) 20 3422 4321
caroline@privacyinternational.org

CERTIFICATE OF SERVICE

I certify that on February 10, 2017, I electronically filed the foregoing brief, as well as the Addendum, with the Clerk of the Court for the United States Court of Appeals for the First Circuit using the appellate CM/ECF system. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by operation of the appellate CM/ECF system.

Dated February 10, 2017

/s/ Caroline Wilson Palow

Caroline Wilson Palow

Privacy International
62 Britton Street
London EC1M 5UY
United Kingdom
+44 (0) 20 3422 4321
caroline@privacyinternational.org

No. 16-1567

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIRST CIRCUIT

UNITED STATES OF AMERICA,
Appellant

v.

ALEX LEVIN,
Defendant-Appellee

Addendum

Table of Contents

1. *United States v. Matish*, No. 16-CR-16, Excerpts of Declaration of Dr. Christopher Soghoian (E.D. Va. June 10, 2016), ECF No. 83-1.....PI.Add.01

2. *United States v. Matish*, No. 16-CR-16, Excerpts of Declaration of Special Agent Daniel Alfin (E.D. Va. June 1, 2016), ECF No. 74-1.....PI.Add.04

3. *United States v. Michaud*, No. 15-CR-5351, Excerpts of Motions Hearing Transcript (W.D. Wa. Jan. 22, 2016), ECF No. 203 .....PI.Add.09

4. *United States v. Michaud*, No. 15-CR-5351, Excerpts of Declaration of Matthew Miller (W.D. Wa. May 9, 2016), ECF No. 191-1 .....PI.Add.16

5. *United States v. Tippens*, No. 16-CR-5110, Excerpts of Evidentiary Hearing Transcript (W.D. Wa. Nov. 1, 2016), ECF No. 103.....PI.Add.18

6. *United States v. Tippens*, No. 16-CR-5110, Excerpts of Declaration of Brian N. Levine, Ph.D. (W.D. Wa. Sept. 22, 2016), ECF No. 58-1.....PI.Add.23

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Newport News Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 4:16cr16
	)	
EDWARD JOSEPH MATISH, III	)	

DECLARATION OF DR. CHRISTOPHER SOGHOIAN

I, Christopher Soghoian, declare the following under penalty of perjury:

1. I am a researcher focused on privacy, computer security and government surveillance. I completed a B.S. in Computer Science from James Madison University, a M.S. in Security Informatics from The Johns Hopkins University and a Ph.D. in Informatics from Indiana University. My academic research has been published in a number of law journals, and has been cited by several federal and state courts, including by the 9th Circuit Court of Appeals and the State Supreme Courts of New Jersey and Massachusetts.[1]

2. I am currently employed by the American Civil Liberties Union as the Principal Technologist in the ACLU's Speech, Privacy and Technology Project. I am also a visiting fellow at Yale Law School's Information Society Project. I have previously worked in technical roles at the Federal Trade Commission, Google, Apple, and IBM. I have written this declaration as an unpaid volunteer expert for the defense and submit it to the court in my personal capacity, not on behalf of my employer.

3. I have researched the FBI's use of Network Investigative Techniques ("NITs") for more than three years. In 2014, I organized the first-ever academic conference in the United States focused on hacking by law enforcement, held at Yale Law School.[2] I have given several public talks about the use of hacking and malware by the FBI, including at training events for federal judges organized by the Federal Judicial Center.

[1] *See US v. Pineda-Moreno*, 617 F. 3d 1120, Court of Appeals, 9th Circuit 2010 (Kozinski dissental), *State v. Earls*, 70 A. 3d 630 - NJ: Supreme Court 2013 and *Commonwealth v. Augustine*, 467 Mass. 230 - Mass: Supreme Judicial Court 2014.

[2] *See* Law Enforcement and Hacking, Information Society Project, Yale Law School, February 18, 2014, videos online at https://www.law.yale.edu/yls-today/yale-law-school-videos/hacking-technologies-used-law-enforcement and https://www.law.yale.edu/yls-today/yale-law-school-videos/legal-and-policy-implications-hacking-law-enforcement .

4. In 2014, while researching the history of FBI hacking, I discovered that in a 2007 operation, FBI agents impersonated the Associated Press in an effort to deliver surveillance software to a teenager in Timberline, Washington. My subsequent public disclosure of this information resulted in significant news coverage, a formal complaint to the Attorney General from twenty-five news organizations,[3] a Congressional probe into the incident,[4] and a public defense of the practice by the FBI Director.[5]

Network Investigative Techniques

5. As Special Agent Alfin's declaration makes clear, there is some disagreement between Michaud's technical experts and the FBI about what a NIT is and is not. There is also clear disagreement about whether or not a NIT is "malware".

6. The term "Network Investigative Technique" was created by the US government. While researching the history of NITs, I was informed by a senior DOJ official that the term originated in the Computer Crime and Intellectual Property Section within DOJ's Criminal Division.

7. Outside of the law enforcement community, a number of terms of art are used by technical security experts to describe software that is installed without the knowledge and consent of a computer user, and that covertly extracts information from that person's computer. These terms include "malware," "surveillance software," and "Remote Administration Tools" (RATs). These terms are all functionally equivalent.

8. In his declaration, Special Agent Alfin suggests, without citing any supporting evidence, that an essential component of malware is that the software must make permanent changes to the security settings of the target computer.[6] I disagree with this statement.

9. The Ninth Circuit Court of Appeals has described malware as software that "works by, for example, compromising a user's privacy… stealing identities, or spontaneously opening Internet links to unwanted websites…." *See Zango v. Kaspersky Lab, Inc., 568 F.3d 1169 (9th Cir. 2009).* Like the malware in *Zango,* the NIT used by the FBI in the Playpen

[3] *See* The Reporters Committee for Freedom of the Press *et al.*, Letter to Eric H. Holder, Jr. and James B. Comey, Jr., November 6, 2014, http://www.rcfp.org/sites/default/files/2014-11-06-letter-to-doj-fbi-regarding-se.pdf
[4] *See* Senator Patrick Leahy, Letter to Eric Holder Jr., October 30, 2014, http://thehill.com/sites/default/files/10-30-14_leahy_to_holder_re_-_fbi_fake_ap_article.pdf.
[5] See James B. Comey, To Catch a Crook: The F.B.I.'s Use of Deception (Letter To The Editor), New York Times, November 5, 2014, http://www.nytimes.com/2014/11/07/opinion/to-catch-a-crook-the-fbis-use-of-deception.html
[6] *See* Alfin Declaration, paragraph 6, page 2.

investigation compromised the privacy and anonymity of the individuals that visited the site, and forced their web browsers to connect to an unwanted site (the FBI's server in Virginia).

10. The capabilities of NITs used by the FBI in other cases include identical surveillance features as malware used by criminals and foreign governments. These capabilities include being able to remotely activate the webcam and microphone on a victim's computer.[7]

11. The FBI has used the same methods as those used by criminal hackers and foreign governments to deliver malware to targets. This includes the impersonation of journalists[8] and the delivery of malware to large numbers of visitors to a particular website (a technique that experts call a "watering hole attack").[9]

12. The primary difference between the FBI's NITs and the malware used by hackers and authoritarian foreign governments appears to be that the FBI's software is used pursuant to court orders issued by a court in the United States. From a technical perspective, the NIT is still malware.

---

[7] Compare the features of BlackShades, a malware tool used by criminals to the capabilities of the NIT software used by the FBI. *See US v. Yücel*, 97 F. Supp. 3d 413 - Dist. Court, SD New York 2015 ("The malware included a remote access tool ('RAT'), which enabled users 'to remotely control victims' computers, including [by] captur[ing] the victims' keystrokes as they type'—the 'keylogger' function— 'turn[ing] on their webcams, and search[ing] through their personal files.'") *See also* Ellen Nakashima and Craig Timberg, FBI's search for 'Mo,' suspect in bomb threats, highlights use of malware for surveillance, Washington Post, December 6, 2013 ("The most powerful FBI surveillance software can covertly download files, photographs and stored e-mails, or even gather real-time images by activating cameras connected to computers, say court documents and people familiar with this technology.")

[8] *See* Bill Marczak and John Scott-Railton, Keep Calm and (Don't) Enable Macros: A New Threat Actor Targets UAE Dissidents, Citizen Lab, Munk School of Global Affairs, The University of Toronto, May 29, 2016, https://citizenlab.org/2016/05/stealth-falcon/ (describing attempts by an entity, believed to be the government of the United Arab Emirates, attemping to deliver malware to dissidents by pretending to be a fictious journalis).

[9] *See* Michael Mimoso, Council on Foreign Relations Website Hit By Watering Hole Attack, IE Zero-Day Exploit, Threatpost, December 29, 2012, https://threatpost.com/council-foreign-relations-website-hit-watering-hole-attack-ie-zero-day-exploit-122912/77352/ . The Department of Justice has taken the position that bulk delivery of NITs in operations like Playpen are not watering hole attacks. As with the question of whether a NIT is malware, the Department of Justice and the technical community do not see eye to eye. *See* David Bitkower, Deputy Assistant Attorney General, Memorandum to Reena Raggi, Chair, Advisory Committee on Criminal Rules, December 22, 2014 http://www.uscourts.gov/file/17944/download at 145 ("The ACLU calls this technique a 'watering hole attack' and suggests that it may violate the Fourth Amendment... The Department disagrees both with that label and with the legal conclusion.")

IN THE UNITED STATES DISTRICT COURT FOR THE

EASTERN DISTRICT OF VIRGINIA

NEWPORT NEWS DIVISION

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 4:16cr16
	)	
EDWARD JOSEPH MATISH, III	)	

DECLARATION OF SPECIAL AGENT DANIEL ALFIN

Your affiant, Daniel Alfin, being duly sworn and deposed, states the following:

1. I am a Special Agent of the Federal Bureau of Investigation. I am currently assigned to FBI Headquarters, Criminal Investigative Division, Violent Crimes Against Children Section, Major Case Coordination Unit. My duties involve the investigation of individuals using various types of technology to produce, distribute, and trade child pornography. As an Agent assigned to the FBI Violent Crimes Against Children Section, Major Case Coordination Unit, I routinely analyze network data that has been collected pursuant to court order. I hold a University Degree in Information Technology and multiple industry certifications that are recognized by the United States Department of Defense. Additionally, I have completed all stages of FBI Cyber Training including courses on Advanced Network Investigative Techniques, Network Traffic Analysis, Ethical Hacking, and Malware Analysis.

2. Analysis of network data generally consists of identifying the origin, destination, and content of communications that are sent across the Internet. In addition to performing this type of analysis, I am routinely called upon to assist Agents across the FBI with similar analysis. In the past two years, I have analyzed data from more than 30 court-authorized network intercepts and those analyses have been used in affidavits and court filings in several judicial districts.

3. I have been involved in the FBI investigation of the Playpen website since it came online in approximately August 2014. Playpen was a website that existed on an anonymous network and was dedicated to the advertisement and distribution of child pornography. My duties included the review of Playpen's content on multiple occasions, engagement in undercover activities on Playpen, and the coordination of investigative activity aimed at identifying members of Playpen, including the defendant, Edward Matish.

4. In preparing this declaration, I have reviewed evidence and spoken with FBI personnel familiar with the facts and circumstances outlined below. I provide the following summary of the information I have learned as a result.

5. I have also reviewed the declaration of Messrs. Tsyrklevich and Miller, the defense experts, respectively dated January 13, 2016 and May 23, 2016, (hereinafter "Tsyrklevich Dec." and "Miller Dec.") and noted a number of statements that are inaccurate and/or require clarification. I will address several of these in great detail below but will begin by noting one overarching misconception in these declarations. Specifically, Tsyrklevich and Miller attempt to redefine the NIT as something containing multiple components. The NIT, however, consists of a single component: that is, the computer instructions delivered to the defendant's computer after he logged into Playpen that sent specific information obtained from his computer back to the FBI. Those computer instructions, and the information obtained via their execution, have been made available for review in this case. In his expert declarations, Matish describes that component as a "payload."

6. As another threshold matter, I would note that I do not consider the NIT used by the FBI to be "malware," though the experts retained by Mr. Matish describe the NIT in such terms. The word malware is an amalgamation of the words "malicious" and "software". The NIT utilized in this investigation was court-authorized and made no changes to the security settings of the target computers to which it was deployed. As such, I do not believe it is appropriate to describe its operation as "malicious."

7. The NIT computer instructions provided to the defense on May 26, 2016 comprise the only "payload" executed on Matish's computer as part of the FBI investigation resulting in his arrest and indictment in this case. Accordingly, the defense has been given access to the only "payload" as that term is used by the defense in the Tsyrklevich declaration.

8. After the NIT collected the information that it was permitted to collect via the computer instructions sent to Matish's computer, there was nothing that resided on Matish's computer that would allow the government (or some other user) to go back and further access that computer.

9. I have personally executed the NIT on a computer under my control and observed that it did not disable the security firewall, make any changes to the security settings on my computer or otherwise render it more vulnerable to intrusion than it already was. Additionally, it did not "infect" my computer or leave any residual malware on my computer.

10. Matish claims via his expert declarations that the NIT consisted of four components – an "exploit," a "payload," software that generates a payload and injects a unique identifier into it, and a server component that stores the delivered information. Tsyrklevich Dec. p. 2 ¶ 4.

11. As used here, a computer "exploit" consists of lines of code that are able to take advantage of a software vulnerability. In layman's terms, an "exploit" could be thought of as a defect in a lock that would allow someone with the proper tool to unlock it without possessing the key. Here, an "exploit" allowed the FBI to deliver a set of instructions-the NIT-to Matish's computer. Those instructions then gathered specified information, including Matish's IP address, and transmitted that information to government controlled computers. The NIT instructions and results have been provided to the defense for review; the "exploit" has not.

12. Tsyrklevich claims that he requires access to the government's "exploit" to determine if the government "executed additional functions outside the scope of the NIT warrant." Tsyrklevich Dec. p. 3, ¶ 6. He is wrong. Discovery of the "exploit" would do nothing to help him determine if the government exceeded the scope of the warrant because it would explain how the NIT was deployed to Matish's computer, not what it did once deployed.

13. The Miller declaration states that "[a] computer system that has been exploited has been fundamentally altered in some way." Miller Dec. p. 2, ¶ 5. Miller cites no authority for that premise. It is incorrect. It is possible for an existing vulnerability in a computer system to be exploited without making any fundamental changes or alterations to that computer system. The Miller declaration also speculates about consequences that may occur "if the security firewall on a computer is disabled by an NIT or other malware." Miller Dec. p. 3, ¶ 7.

14. It is theoretically possible for an exploit to make fundamental changes or alterations to a computer system or to disable its security firewall. However, as noted above, the NIT used here and the exploit used to deliver it did not do so. Other than to point to this theoretical possibility, I am aware of no evidence or indication to which either defense expert points to suggest otherwise.

15. The government has advised the defense that it is willing to make available for its review the two-way network data stream showing the data sent back-and-forth between Matish's computer and the government-controlled computer as a result of the execution of the NIT.

16. Review of this data stream reflecting the information transmitted to the FBI from Matish's computer as a result of the deployment of the NIT confirms that the data sent from Matish's computer is identical to the data the government provided as part of discovery.

17. Review of the network data stream also confirms that that no images were transmitted from Matish's computer to a government-controlled computer or from a government-controlled computer to Matish's computer as a result of the execution of the NIT.

18. Discovery concerning the "server component" is unnecessary because there are alternative means of verifying the accuracy of the NIT information.

19. Tsyrklevich claims that he needs access to the server component in order to confirm that the information obtained from Matish's computer by the NIT and sent to the FBI was accurately stored and reproduced. Tsyrklevich Declaration pp. 3-4. The defense does not need access to government servers to do this, however, because the government has agreed to provide an alternative method of verifying that the information obtained from Matish's computer was accurately recorded. Specifically, the government has offered to provide a copy of the data stream sent by Matish's computer to the government as a result of the execution of the NIT. Tsyrklevich can compare the information sent to the government by the NIT to the information provided in discovery to verify that what the government recorded from Matish's computer is in fact what was sent by Matish's computer. I have reviewed that data stream and, as explained below, confirmed that the information sent by Matish's computer as a result of the NIT matches the information that is stored on the government's servers.

20. When two computers communicate via the Internet, they do so using standard network protocols. Communications over the Internet are sent in "packets," which serve as the means by which computers share information over a network. Just as two people communicating over email exchange individual messages, computers exchange network packets. These packet exchanges follow standard network protocols that permit individual computers to process and exchange information with one another. Just like two people meeting on the street, computers wishing to communicate with one another first exchange greetings through a "handshake,"[1] then exchange information, and part ways with a communication exchange that basically consists of the computers saying "goodbye" to each other.

21. Here, when the NIT was delivered to Matish's computer, it had exactly this sort of interaction with a government-controlled computer. The network packets memorializing this exchange, which have been preserved in a standard file format, make it possible to reconstruct that exchange and see exactly what information was transmitted by Matish's computer to the government.

22. A review of the data file, known as a PCAP file, documenting the exchange contains several network packets exchanged between Matish's computer and the government computer. The initial packets correspond to the initial "handshake" that established the connection between Matish's computer and the government computer. Similarly, the final packets in the

[1] Some protocols that are used to communicate via the Internet do not include a "handshake" as described in this declaration. These other protocols are not relevant to the matter at hand as the communications that occurred as a result of the deployment of the NIT did utilize a network protocol that included a "handshake".

communication correspond to the "goodbye" communication between the two computers. The remaining packet(s) thus contains the substance of the communication, namely, the information collected by the NIT after it was delivered to Matish's computer.

23. Reviewing these packets, I was able to confirm that the information collected from Matish's computer matches the information stored on the government servers that has been provided in discovery. Each of the pieces of information the government-controlled computer recorded being collected from Matish's computer by the NIT appears in the packets. If Tsyrklevich's goal is to verify the accuracy of the information stored by the government, then a review of the network data is all that would be required. The data is not encrypted or redacted thus making such a review possible.

24. Tsyrklevich maintains that he needs access to the computer code that "generates a payload and injects a unique identifier" in order to ensure the identifier used was in fact unique. Tsyrklevich Dec. p. 3 ¶ 6. He is wrong because the unique identifier assigned to Matish's NIT results was in fact unique.

25. Prior to deployment of the NIT, a unique identifier is generated and incorporated into the NIT. When the "activating computer"' sends information to the government as a function of the NIT, that unique identifier is included with the response. When the information is received by the government, a check is performed to ensure that the unique identifier contained within the delivered information matches the unique identifier that was generated by the government. In the matter at hand, all identifiers received by the government, including the one sent by Matish's computer, did match identifiers that were generated by the government and they were in fact unique.

26. The ultimate question posed by Tsyrklevich is not how the unique identifier was generated but if the unique identifier sent to Matish's computer was actually unique. I have reviewed the list of unique identifiers generated during the operation and confirmed that there were in fact no duplicate identifiers generated.

27. A query of an FBI database containing the information gathered as part of this investigation through the use of the NIT revealed the following: 1) there are no duplicate unique identifiers within the database, meaning that each identifier assigned to an individual Playpen user is in fact unique; 2) the identifier associated with the username "Broden" was in fact unique; and 3) there are no identifiers in the database other than those generated by the deployment of a NIT as part of this investigation; the significance of which is the fact that this proves no outside entity tampered with or fabricated any of the unique identifiers generated as part of the investigation.

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
IN TACOMA

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	No. CR15-5351RBJ
	)	
vs.	)	
	)	
JAY MICHAUD,	)	
	)	
Defendant.	)	

MOTIONS HEARING

BEFORE THE HONORABLE ROBERT J. BRYAN
UNITED STATES DISTRICT COURT JUDGE

January 22, 2016

APPEARANCES:

Keith Becker
U.S. Department of Justice Criminal Division
Matthew Hampton
Assistant United States Attorney
Representing the Plaintiff

Colin Fieman
Linda Sullivan
Federal Public Defender's Office
Representing the Defendant

EXAMINATION INDEX

EXAMINATION OF		PAGE
DANIEL ALFIN	DIRECT EXAMINATION	54
	By Mr. Becker	
	CROSS-EXAMINATION	73
	By Mr. Fieman	
	REDIRECT EXAMINATION	89
	By Mr. Becker	
	RECROSS-EXAMINATION	94
	By Mr. Fieman	
CHRIS SOGHOIAN	DIRECT EXAMINATION	99
	By Mr. Fieman	
	CROSS-EXAMINATION	120
	By Mr. Becker	
	REDIRECT EXAMINATION	128
	By Mr. Fieman	

EXHIBIT INDEX

EXHIBITS ADMITTED	PAGE
12A	57
12B	58
15	62
15B	63
13B	71
13A	91
1 - 9	97
A15 & A16	98

11:52:13AM **Q. So at some point some FBI agent or tech specialist**
11:52:18AM **set up the NIT to be activated when somebody signed in,**
11:52:23AM **correct?**
11:52:24AM **A. That's correct.**
11:52:25AM **Q. And at the point that the person is signing in, and**
11:52:30AM **the NIT is being activated, you don't have that telephone**
11:52:33AM **number or complete IP address, correct? That's what you**
11:52:36AM **want to get?**
11:52:37AM **A. Prior to a user logging into the website, and prior**
11:52:40AM **to the NIT being activated, we do not have any identifying**
11:52:44AM **information, including an IP address, for that user.**
11:52:48AM **Q. Correct. And the way the NIT works is that it is**
11:52:53AM **then sent, without the user's knowledge, from the site in**
11:52:57AM **Virginia to the user's computer, wherever that may be,**
11:53:02AM **correct?**
11:53:02AM **A. The user after certain conditions are met --**
11:53:05AM **Q. Such as signing in?**
11:53:06AM **A. Correct. As articulated in the warrant.**
Q. Yes.
11:53:10AM **A. And in the case of this defendant, accessing a**
11:53:13AM **particular post on the website. By accessing that post on**
11:53:18AM **the website, that user has triggered actions that causes**
11:53:21AM **his computer to download certain information from the**
11:53:23AM **website. We configured the NIT to supplement the**
11:53:26AM **information being downloaded by the user with the NIT**

11:53:30AM instructions.
11:53:31AM Q. Okay. And, again, I need to go really slowly because
11:53:35AM already we are using words like "supplement" that are a
11:53:37AM little confusing. Just step-by-step. The user has signed
11:53:41AM in, the FBI has set it up so the NIT will be deployed at
11:53:47AM sign in, or at some other point, correct?
11:53:50AM A. After certain conditions are met, yes.
11:53:53AM Q. Then that NIT is really like a package of code or
11:53:56AM data, right?
11:53:57AM A. Yes.
11:53:58AM Q. And when the user is signing in, they don't know that
11:54:03AM they are getting that package of code or data sent to
11:54:06AM them, right? The whole point is it is in the background,
11:54:09AM and secret?
11:54:10AM A. When the user downloads the NIT instructions to their
11:54:13AM computer, it is intended to be invisible to the user.
11:54:16AM Q. It is invisible. Okay. They are signing in and then
11:54:19AM all of a sudden this thing in the background --
11:54:22AM information is being sent from Virginia, to, in this case,
11:54:24AM a Washington computer, by the FBI?
11:54:26AM A. It is being downloaded from the server in the Eastern
11:54:30AM District of Virginia by the user who has accessed the
11:54:33AM website.
11:54:33AM Q. How does the NIT code get from Virginia to
11:54:39AM Washington? It travels, right?

01:44:40PM within that web page would have been an instruction for
01:44:43PM the Tor browser -- not for the defendant, but for the Tor
01:44:47PM browser.
01:44:47PM Q. Let's stop there. When you say "contained," can you
01:44:50PM see that on the web page?
01:44:52PM A. Can a human see it?
01:44:54PM Q. Would the user who is looking for, say, a picture on
01:44:58PM the internet, would they see those instructions?
01:45:01PM A. No, there wouldn't have been any instructions visible
01:45:03PM to a regular user. A high-tech sophisticated person might
01:45:08PM be able to figure that out, but a regular person just
01:45:11PM clicking around is not going to know there has been this
01:45:14PM new special code added to the web page.
01:45:17PM Q. So it is hidden code running in the background. When
01:45:20PM you say "sending instructions," it is not instructions to
01:45:22PM the user, in this case allegedly Mr. Michaud, it is
01:45:26PM instructions to the target computer?
01:45:28PM A. I want to pause on that word "running." The code
01:45:31PM does not run on the website. The code always runs on your
01:45:36PM web browser. So the website tells the web browser, "Do
01:45:39PM this." The code is downloaded to the web browser, the Tor
01:45:42PM browser in this case, in this case in the state of
01:45:45PM Washington. And it is only when the instructions are
01:45:47PM received by the Tor browser here in the state of
01:45:50PM Washington that they are run on that computer, and then do

links the computer to a residential internet account. It would be what is called the MAC address, which is a unique serial number associated with your wi-fi card, programmed in the factory of the wi-fi card manufacturer. There would be some other information about the operating system that the special agent read out when he was on the stand, the user name on the computer, which version of Windows you are running, some basic information.

But to learn that information, before the NIT could transmit that information back to the computer in Virginia, it would first have to go and collect it. So if you think of this as information that is in a house, well, maybe one piece of it is in the bedroom, and another piece is in the living room, one piece of it is in the drawer. The NIT first has to go and collect the information from different parts of the computer. And then once it has that information, then it would transmit it back to the server in Virginia.

Q. So if I understand the process, the NIT bypasses security or overrides security features on the Washington computer. First step, right? And then second, it actually collects data or evidence on that computer. And then the third step, after it has seized the Washington data in this case, it then wraps it up in like a little evidence bag and delivers it to the FBI in Virginia?

01:49:45PM A. That sounds right. Although I'm not sure about the
01:49:49PM evidence bag. It transmits it back to the computer in
01:49:52PM Virginia.
01:49:52PM Q. And then once that data has been transmitted back, it
01:49:57PM is stored, apparently, on an FBI server; is that correct?
01:50:01PM A. The special agent said that the server is under the
01:50:06PM government's control. I am not sure how much I can say in
01:50:10PM this room about where we think the server is or which
01:50:13PM company we think might have been running the server.
01:50:15PM Q. I don't want you to --
01:50:17PM A. A computer in Virginia.
01:50:20PM Q. Is it then fair to say after this search and seizure
01:50:24PM in Washington, then really what is going on is it is in
01:50:26PM like an evidence room in Virginia where they keep that
01:50:28PM evidence until they need it?
01:50:31PM MR. BECKER: Object to leading at this point, your
01:50:33PM Honor. I think we are just reiterating testimony.
01:50:34PM THE COURT: That is a fair objection.
01:50:36PM By Mr. Fieman:
01:50:36PM Q. Describe then what the storage in Virginia is about.
01:50:38PM A. Once the data has been transmitted by the NIT, I have
01:50:43PM no idea what the government would do with it. We know
01:50:46PM that it was transmitted to a computer in Virginia. At
01:50:49PM that point we have no -- They haven't turned over
01:50:51PM information about how it is stored, or who has access to

JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	No. CR15-5351RJB DECLARATION OF MATTHEW MILLER

I, Matthew Miller, declare under penalty of perjury that:

1. I am an Assistant Professor of Computer Science and Information Technology at the University of Nebraska at Kearney. A copy of my CV is attached to this declaration. Based on my prior work analyzing FBI "Network Investigative Techniques," I have been retained by Mr. Michaud's defense team to speak to the importance of analyzing **all** source code used by the FBI in the deployment of a NIT.

2. As explained in the declaration of Vlad Tsyrklevich that has been previously presented to the Court, an NIT has four major components. Each of these components must be reviewed and verified by the defense for three basic reasons. First, to ensure that the evidence collected by the NIT is valid and accurate. Second, to ensure that the FBI's use of its NIT did not exceed what was authorized in the NIT search warrant, which is an emerging and serious problem with different types of sophisticated search and seizure technology now used by law enforcement agencies. Third, to develop potential defenses at trial based on the NIT having compromised the security settings on Mr. Michaud's computer and rendering it vulnerable to a host of viruses and

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

remote attacks that would explain to a jury why a defendant's data storage devices may contain child pornography that he or she did not intentionally download.

3. As the Court is aware, under normal circumstances the FBI would be able to target a specific user on the Internet by using their Internet Protocol (IP) address. This address identifies a user and is allocated to an Internet Service Provider (ISP). The ISP can identify each of their users and then the FBI can investigate that single user. When users use Tor, they are "anonymized" such that the FBI cannot readily identify them by their IP address because that IP address is not transmitted or shared in any retrievable way. The FBI must use an "exploit" in the software that the user is running on his or her computer to seize the IP address and other identifying information from that target computer directly. An exploit is a piece of software that takes advantage of a flaw in a computer system. Among other components, the FBI has not produced the exploit that was used in this case.

4. A computer system that has been exploited has been fundamentally altered in some way. This alteration may cause the computer to crash, lose or alter data, not respond to normal input or it may alter **any of the settings on that system.**[1] Depending on the exploit, it can affect the security posture of the computer going forward.[2]

5. Once a computer system's security has been compromised, the computer and any devices that have been connected to it (such as thumb drives, discs or other data storage devices) are also deemed to have been compromised and vulnerable to attack. As a result, the distinction the government has been trying to draw in various

---

[1] C. Smith, Dangerous Windows 10 flaw lets hackers secretly run any app on your PC, http://bgr.com/2016/04/25/windows-10-applocker-security-issue/, 2016.

[2] D. Goodin, New exploit leaves most Macs vulnerable to permanent backdooring, http://arstechnica.com/security/2015/06/new-remote-exploit-leaves-most-macs-vulnerable-to-permanent-backdooring/, 2015.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, vs. DAVID TIPPENS, Defendant.	Docket No. CR16-5110RJB Tacoma, Washington November 1, 2016
UNITED STATES OF AMERICA, Plaintiff, vs. GERALD LESAN, Defendant.	Docket No. CR15-387RJB
UNITED STATES OF AMERICA, Plaintiff, vs. BRUCE LORENTE, Defendant.	Docket No. CR15-274RJB

TRANSCRIPT OF EVIDENTIARY HEARING CONTINUED
BEFORE THE HONORABLE ROBERT J. BRYAN
SENIOR UNITED STATES DISTRICT COURT JUDGE

Court Reporter: Teri Hendrix
Union Station Courthouse, Rm 3130
1717 Pacific Avenue
Tacoma, Washington 98402
(253) 882-3831

Proceedings recorded by mechanical stenography, transcript produced by Reporter on computer.

APPEARANCES:

For the Plaintiff:	MATTHEW HAMPTON Assistant United States Attorney 700 Stewart Street, Suite 5220 Seattle, Washington 98101-1271
	KEITH BECKER U.S. Department of Justice 1400 New York Avenue NW, 6th Floor Washington, DC 20530
For Defendant Tippens:	COLIN FIEMAN Office of the Public Defender 1331 Broadway, Suite 400 Tacoma, Washington 98402
For Defendant Lesan:	ROBERT W. GOLDSMITH Law Office of Robert W. Goldsmith 702 2nd Avenue Seattle, Washington 98104
For Defendant Lorente:	MOHAMMAD ALI HAMOUDI Office of the Public Defender 1601 5th Avenue, Suite 700 Seattle, Washington 98101

government is not slipping things by magistrate judges or exceeding their powers without comprehensive judicial oversight. So will the courts require the FBI to be candid and transparent going forward? Will the government be required to follow the rules even if they disagree with them because we live by the rule of law?

When it comes to law enforcement, are we going to start saying the ends justify the means, no matter the collateral consequences or the revictimization that's involved? These are core principles of our judicial system that I believe are seriously implicated in this case. If there aren't some bright lines laid down, then the technology and the secrecy is going to simply get away from us.

Now, what do we know now, Your Honor, six months after the *Michaud* ruling. Every time Your Honor grants a discovery request and we get new information, it's like -- to use an appropriate metaphor, like peeling an onion. There's just another layer of fact there that we did not know about. I mean, we did not know this was a truly global warrant before. There are 120 countries and territories listed outside the United States that the FBI hacked into, and they also hacked into something called a "satellite provider." So now we are into outer space as well.

Now, they did that -- and we've submitted this as an exhibit in our supplemental discovery. They did this in spite

the motion to exclude on the discovery issue related to what the government's expert testified to yesterday. He used two analogies, Your Honor, that I think we can use to support our position. One is that he argued that in a burglary case, you would be concerned with two things: How the burglar got into the house, and what happened after the burglar was there.

The exploit is -- to analogize -- is how the burglar got into the house. And in any burglary case, someone would have to prove both of those things, how the burglar got in and then what happened afterwards. We are being deprived of the evidence regarding how the burglar got in, so to speak.

Going further, their expert analogized the exploit to a key, something that sounds very simple, but he didn't examine the exploit. He agreed he did not see it, he does not know what that code is. And he's coming up with an argumentative analogy: What if that exploit isn't a key, but it's a battering ram? What if it's something that blows the door off of the computer? We don't know that. And that's why it's relevant to the defense, particularly in the search context. So I want the Court to think about that as well.

In terms of the search issues themselves, just last week on October 26th, the government sent us some discovery. And interestingly, there were a couple of memos where the FBI was explaining what this investigation was, and I am going to read just the beginning sentence from that -- those two memos, and

it's the same in each memo.

It says: "Operation Pacifier is an international investigation into a Tor hidden service known as Playpen and its users." The key word there, Your Honor, is "international." Nowhere in any of the warrant documents, the application, the warrant face itself, do they use that word "international." How is a magistrate judge to know, when they know their investigation is international and they never once use that word, the only word that we've heard already is buried on page 29, paragraph 45, that the computers wherever located. That's it. We know under Ninth Circuit law, that particular line cannot expand the warrant. That line cannot expand the warrant. Ninth Circuit law is very strict on interpreting warrants. It was not a magistrate error.

Secondly, some of the additional information they gave -- and I think the Court heard these numbers. There were approximately 8,713 IP addresses derived during this investigation. That's something we learned just late last week. Of those 8,713, 7,281 of them were foreign. So the vast majority, something like 84 percent of the actual materials they got through the NIT, were not on U.S. soil. This was really a truly international warrant, and they never used that word.

Your Honor, it is very clear to me that the government was not engaging in their duty of candor with that magistrate.

The Honorable Robert J. Bryan

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. DAVID TIPPENS, Defendant.	NO. CR16-5110 RJB **DECLARATION OF BRIAN N. LEVINE, Ph.D.**
UNITED STATES OF AMERICA, Plaintiff, v. GERALD LESAN, Defendant.	NO. CR15-387 RJB **DECLARATION OF BRIAN N. LEVINE, Ph.D.**
UNITED STATES OF AMERICA, Plaintiff, v. BRUCE LORENTE, Defendant.	NO. CR15-274 RJB **DECLARATION OF BRIAN N. LEVINE, Ph.D.**

that contract. My work is being performed pursuant to a contract with the U.S. Attorney's Office for the Western District of Washington.

2. In preparing this declaration, I have reviewed the following: from *U.S. v. Michaud*, No. CR15-5351RJB, the declaration of Vlad Tsyrklevich dated January 13, 2016 (hereinafter "Tsyrklevich Dec."), the declaration of Robert Young dated May 2, 2016 (hereinafter "Young Dec."), the declaration of Shawn Kasal dated May 9, 2016 (hereinafter "Kasal Dec."), and the declaration of Dr. Matthew Miller dated May 9, 2016 (hereinafter "Miller Dec."); the declaration of Special Agent Daniel Alfin from *U.S. v. Matish*, No. 4:16cr16 filed June 1, 2016 (hereinafter "Alfin Dec."); the network packet capture (PCAP) evidence from the computers of Tippens, Lesan, and Lorente, and the corresponding FBI payload executables for each; excerpts of the Cygnus report for Tippens, Lesan, and Lorente that contain the FBI's recording of information collected by the NIT for each of their computers; the forensic examination reports for the devices of Lorente dated February 28, 2016, Lesan dated December 20, 2015, and Tippens dated July 11, 2016; the NIT warrant application (*In the Matter of the Search of Computers that Access upf45jv3bziuctml.onion*, Case No. 1:15-SW-89 Eastern District of Virginia); and the complaint against Tippens dated February 11, 2016. I am advised that all of that information has been disclosed to or made available to the defendants for review.

3. I have not had access to nor did I review the source code or executable for the FBI exploit that deployed the NIT payloads. I also have not had access to nor did I review the FBI server or any "generator" code used to create unique identifiers.

4. Based on my review of available documents, my understanding of the overall process used by the FBI is as follows. A defendant's computer connected using the Tor network to the Playpen website, logging in with a specific username. Retrieving certain pages from the Playpen website resulted in the download of the FBI's *exploit* and *payload* programs. Much like a tool to open a locked door to a house, the purpose of the exploit was to allow for the execution of the payload program on a defendant's computer. The bespoke payload carried a *unique identifier* that was generated by the FBI, as well as

a *case identifier* common to all payloads generated for the Playpen operation. The payload program queried a defendant's computers for certain information, such as the hostname and operating system type. These details, along with the unique identifier and case identifier were sent by the payload program to an FBI server via the Internet. The action of sending data to the FBI over the Internet revealed the public IP address used by the defendants that was assigned by an Internet Service Provider (ISP) and linked to billing information. The exploit and payload did not persist on the defendants' computers after execution.

5. In this document, my references to "the exploit", "payload", "generator", "NIT", and "server" are reserved to the mechanisms employed by the FBI. My use of the term "malware" is reserved for computer programs that were created or deployed by third parties (i.e., neither the defendants nor the FBI) intending harm by, for example, downloading images of child sexual abuse to a computer unbeknownst to its owner.

6. From the materials available to me, I have concluded the following.

a. When viewed in the context of the facts of these cases, the declarations of Messrs. Tsyrklevich, Miller, Kasal, and Young contain many overbroad generalizations and implausible explanations, which are not rooted in cited or documented facts or evidence, and they are insufficient to support their hypotheses.

b. Specifically, *there is no evidence to support any of the following hypotheses* referenced in the defendants' submissions: the defendants did not visit the Playpen website; the information relayed by the payload to the FBI servers via the Internet was tampered with or altered by a third party; the identifiers generated by the FBI are not reliable; an FBI exploit or payload made permanent changes to the security settings or any other settings of the defendants' computers; an FBI exploit or payload are responsible for images of child sexual abuse found on the defendants' computers and in their residences.

c. A review of the exploit, software that generated unique identifiers, or server software is not necessary to show that these hypotheses are merely speculation