No. 17-30117

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

DAVID TIPPENS,

Defendant-Appellant.

On Appeal from the United States District Court for the
Western District of Washington at Tacoma District Court

BRIEF OF *AMICUS CURIAE* PRIVACY INTERNATIONAL IN SUPPORT OF DEFENDANT-APPELLANT AND REVERSAL

Scarlet Kim
Counsel for Amicus Curiae

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

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rules of Appellate Procedure 26.1 and 29(a)(4)(A), *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 iii

STATEMENT OF INTEREST 1

INTRODUCTION 2

FACTUAL BACKGROUND 4

I. The "Network Investigative Technique." 4

A. The NIT uses an "exploit" and a "payload." 4

B. The NIT sends an exploit to devices in bulk. 7

C. The NIT deploys the exploit to compromise the security of devices. 9

D. The NIT runs a "payload" to perform actions on the compromised devices.11

ARGUMENT 12

I. THE NIT WARRANT IS INVALID BECAUSE IT AUTHORIZED EXTRATERRITORIAL SEARCHES AND SEIZURES. 12

A. International law prohibits unilateral extraterritorial searches and seizures. 13

B. Rule 41 does not authorize extraterritorial searches and seizures. 17

C. The magistrate judge lacked authority under Rule 41 to issue the NIT warrant because it authorized extraterritorial searches and seizures. 19

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

TABLE OF AUTHORITIES

Federal Cases

United States v. Gorshkov, No. 00-cr-550, 2001 WL 1024026 (W.D. Wash., May 23, 2001) 25

United States v. Werdene, 188 F.Supp.3d 431, 440 (E.D. Pa. 2016) 12

International Cases

Arrest Warrant of 11 April 2000 (Dem. Rep. Congo v. Belg.) 2002 I.C.J. 3 (Feb. 14) 15

SS Lotus (Fr. v. Turk.) 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7) 14, 15

Statutes and Rules

18 U.S.C. §1030(a)(2) 25

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

Other Authorities

Michael Abbell, *Obtaining Evidence Abroad in Criminal Cases* (2010) 23

Michael Akehurst, *Jurisdiction in International Law*, 46 Brit. Y. B. Int'l L. 145 (1975) 15

Patricia L. Bellia, *Chasing Bits across Borders*, U. Chi. Legal F. 35 (2001) 17

Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 Nw. J. Tech. & Intell. Prop. 1 (2014) 4-5, 9, 11

Sam Biddle, *Can 000000 Secretly Open Your Hotel Safe?*, Gizmodo (Sept. 6, 2011), http://gizmodo.com/5837561/can-000000-secretly-open-your-hotel-safe 5

Susan W. Brenner, *Cyber-threats and the Limits of Bureaucratic Control*, 14 Minn. J.L. Sci. & Tech. 137 (2013) 24

Ian Brownlie, *Principles of Public International Law* (8th ed. 2012) 15

Mike Brunker, *FBI agent charged with hacking*, NBC News (Aug. 15, 2002), http://www.nbcnews.com/id/3078784 25

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) 25

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

Council on Europe, Convention on Cybercrime, *opened for signature* Nov. 23, 2004, S. Treaty Doc. No. 108-11 (2006), 2296 U.N.T.S. 167 (entered into force July 1, 2004) 16, 17, 22-23

James Crawford, *Brownlie's Principles of Public International Law* (8th ed. 2012) 17-18

Robert Cryer et al., *An Introduction to International Criminal Law and Procedure* 44 (2d ed. 2010) 14

Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale L.J. 326 (2015) 17, 18

Dep't of Justice, Office of International Affairs, https://www.justice.gov/criminal-oia 23

Dep't of Justice, U.S. Attorney's Manual, Criminal Resources Manual 21, 24

Dep't of State, Foreign Affairs Manual 22

Charles Doyle, Cong. Research Serv., *Extraterritorial Application of American Criminal Law* (2016) 22

The Draft Convention on Research in International Law of the Harvard Law School, 29 Am. J. Int'l L. 435 (Supp. 1935) ... 13

T. Markus Funk, Fed. Judicial Ctr., *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges* (2014) ... 22

Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 Stan. L. Rev. 1075 (2017) ... 23

Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 Cal. L. Rev. 817 (2012) ... 16

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 ... 5, 6

Int'l Bar Ass'n, *Report of the Task Force on Extraterritorial Jurisdiction* (2009) ... 14

The Jargon File (Oct. 1, 2004), http://www.catb.org/jargon/index.html ... 6

Henrik W.K. Kaspersen, Council of Europe, *Cybercrime and Internet Jurisdiction* (2009) ... 16

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/ ... 8

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) ... 8

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) ... 18, 19

Terminology, Malware Attribute Enumeration and Characterization, MITRE (Jan. 2, 2014), http://maec.mitre.org/about/terminology.html ... 6-7

Frederick A. Mann, *The Doctrine of Jurisdiction in International Law* (1964) 13-14

The New Hacker's Dictionary (Eric S. Raymond ed., 3d ed. 1996) 6

Lassa Oppenheim, *Oppenheim's International Law* (Robert Jennings & Arthur Watts eds., 9th ed. 1992) 13

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/ 6

Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, delivered to the General Assembly, U.N. Doc. A/70/174 (July 22, 2015) 15-16, 24

Restatement (Third) of Foreign Relations Law in the United States (Am. Law Inst. 1987) 13, 14, 17

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Michael N. Schmitt ed. 2017) 15, 17

Tor: Overview, Tor, https://www.torproject.org/about/overview.html.en (last visited Feb. 3, 2017) 9

Tor: Hidden Service Protocol, Tor, https://www.torproject.org/docs/hidden-services.html.en 9-10

Tor: Metrics, Tor, https://metrics.torproject.org/userstats-relay-table.html?start=2015-02-01&end=2015-02-28 20

What is Tor Browser?, Tor, https://www.torproject.org/projects/torbrowser.html.en 9

Matthew C. Waxman, *Self Defense Force Against Cyber Attacks*, 89 Int'l L. Stud. 109 (2013) 24

STATEMENT OF INTEREST

Privacy International is a non-profit, 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* states 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. In particular, it possesses the capability to search and seize data from connected devices located anywhere in the world. The NIT's extraterritorial reach was clear to the government when it sought authority to deploy this technology. And we now know that the NIT infiltrated over 8,700 devices, over 83% of which were located outside of the U.S., in 120 countries and territories.

The NIT warrant therefore ostensibly 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 there is no evidence the government sought 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's extraterritorial reach renders the warrant invalid and potentially subjects the U.S. to profound foreign relations risks. For these reasons, this Court should reverse the district court's denial of David Tippens's motions to suppress.

FACTUAL BACKGROUND

I. The "Network Investigative Technique."

The NIT comprises multiple distinct processes, involving the use of distinct technical components. These processes render the NIT a technique to:

(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.[2]

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

A. 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.[3] *See* Steven M. Bellovin et al., *Lawful*

[2] Privacy International relies primarily on expert declarations and testimony to describe the NIT. Several of these statements form part of the record in this case. These statements were elicited in conjunction with motions to compel discovery regarding the NIT or exclude evidence derived from the NIT pursuant to Federal Rule of Criminal Procedure 16(d). They currently constitute the most detailed technical information in the public domain about how the NIT operates.

[3] 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* Decl. of Brian Levine, *United States v. Tippens*, No. 16-cr-5110 (W.D. Wa. Sept. 22, 2016), ECF No. 58-1, ¶4 ("[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* Decl. of Special Agent Daniel Alfin, *Tippens*, (Sept. 22, 2016), ECF No. 62, ¶11 ("[A]n 'exploit' allowed the FBI to deliver a set of instructions – the NIT – to [the

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 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.

defendant]'s computer. . . . The NIT instructions and results have been provided to the defense for review; the 'exploit' has not."). Experts for the appellant in the underlying proceedings as well as scholars following this wave of litigation agree that the exploit constitutes a component of the NIT. *See, e.g.*, Decl. of Vlad Tsyrklevich, *Tippens* (Aug. 22, 2016), ECF No. 31-2, ¶4 (ER.S.VI 1113) (describing the "exploit" as one of "four primary components" of the NIT); Decl. of Matthew Miller, *Tippens* (Aug. 22, 2016), ECF No. 31-3, ¶¶3-4 (ER.S.VI 1118) (agreeing with Tsyrklevich's description); 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).

The unsealed volumes of the Excerpts of Record are cited as "ER.[Vol.]". The sealed volumes of the Excerpts of Record are cited as "ER.S.[Vol.]". The citations to the sealed volumes are to documents that are available in public filings in the underlying proceedings as well as other criminal proceedings arising out of the government's execution of the NIT warrant. Appellant's counsel has provided Privacy International with the page numbers in the sealed volumes for these documents for citation purposes.

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.[4] 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), http://www.catb.org/jargon/index.html (entry for "malware").[5] 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),

[4] Experts for the government do not dispute that it used a payload. *See, e.g.* Levine Decl. ¶4; Alfin Decl. ¶7. 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 Surreply to Def. Mot. to Compel Discovery at 11-12, *United States v. Matish*, No. 16-cr-16 (E.D. Va. June 1, 2016), ECF No. 74. Nevertheless, computer security experts have used this term to describe the NIT. *See* Decl. of Dr. Christopher Soghoian, *Matish,* (June 10, 2016), ECF No. 83-1 ¶¶5-12; 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).

[5] 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., 3d ed. 1996).

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.

B. 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 (ER.S.V 946). 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 (ER.S.V 946). 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.*; *see also* Motions Hearing Tr., *United States v. Michaud*, No. 15-cr-5351 (W.D. Wa. Jan. 22, 2016), ECF No. 203 (ER.S.VI 1159) (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 (ER.S.V 946), is, as clarified by one of its own experts, instructions to send an exploit. Levine Decl. ¶4 ("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 (ER.S.V 940). 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 (ER.S.V 946). 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.[6]

[6] 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 ("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).

C. 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.[7] *See* Tsyrklevich Decl. ¶4 (ER.S.VI 1113); *see also* Mozilla Motion 4 (ER.IV 563) ("[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 Oct. 14, 2017). Through the Tor Browser, users can connect to the Tor network, which protects their anonymity while using the internet. *See Tor: Overview*, Tor, https://www.torproject.org/about/overview.html.en (last visited Oct. 14, 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-

[7] 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 ("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 (ER.IV 563) ("[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").

services.html.en (last visited Oct. 14, 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 evade the security protections of the Tor Browser, which normally prevent websites from determining certain identifying information of visitors. *See* Tsyrklevich Decl. ¶4 (ER.S.VI 1113). More broadly, however, by circumventing the security protections of the Tor Browser, the exploit compromised the security of the devices themselves.[8] *See* Motions Hearing Tr. 115-16 (Soghoian Test.) (ER.S.VI 1162-63) ("Q. [T]he NIT bypasses security or overrides security features on the [target] computer. . . . A. That sounds right."); Mozilla Motion 3 (ER.IV 562) ("Mozilla has reason to believe that the Exploit . . . is an active vulnerability in its Firefox code base that could be used to compromise users and systems running the browser.").

[8] 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 (emphasis added); Levine Decl. ¶6(b) (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).

D. 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.[9] *See* Tsyrklevich Decl. ¶4 (ER.S.VI 1113) ("After exploiting the vulnerability, the NIT delivers a software 'payload.'"). 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 (ER.S.V 946-47) (listing the information sought by the government). The payload was further designed to copy and transmit that information from the device to the government. *See* Tsyrklevich Decl. ¶4 (ER.S.VI 1113) ("The payload used by the FBI in this case collected and transmitted identifying information about the host computer.").

[9] In part because the exact nature of the exploit remains unclear, *see supra* note 7, 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.*

ARGUMENT

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

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 United States v. Werdene*, 188 F.Supp.3d 431, 440 (E.D. Pa. 2016) (citing cases). But absent from this debate is a consideration of the extraterritorial jurisdictional limitations on the warrant authority. These limitations are just as pertinent to an evaluation of the scope of Rule 41 in this case. The government has 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 (ER.III 326). Specifically, the NIT returned 8,713 IP addresses, 7,281 (over 83%) of which were foreign. *Id*. at 39 (ER.III 347). Below, Privacy International discusses the international and domestic legal bases for extraterritorial jurisdictional limitations on the warrant authority. Privacy International further describes the foreign relations implications of breaching these limitations.

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). Jurisdiction refers to "the authority of states to prescribe their law, to subject persons and things to adjudication in their courts . . . and to enforce their law." *Id*. at pt. IV, Introductory Note; *see also* Lassa Oppenheim, *Oppenheim's International Law* 456 (Robert Jennings & Arthur Watts eds., 9th ed. 1992); *The Draft Convention on Research in International Law of the Harvard Law School*, 29 Am. J. Int'l L. 435, 467-69 (Supp. 1935). Jurisdiction is inextricably linked to the principles of sovereignty and territoriality:

> Jurisdiction is an aspect of sovereignty, it is coextensive with and, indeed, incidental to, but also limited by, the State's sovereignty. As Lord Macmillan said, "it is an essential attribute of the sovereignty of this realm, as of all sovereign independent States, that it should possess jurisdiction over all persons and things within its territorial limits and in all cases, civil and criminal, arising within these limits". If a State assumed jurisdiction outside the limits of its sovereignty, it would come into conflict with other States which need not suffer any encroachment upon their own sovereignty . . . . Such a system . . . divides the world into compartments within each of which a sovereign State has jurisdiction.[10]

Frederick A. Mann, *The Doctrine of Jurisdiction in International Law* 30 (1964).

[10] The principle of sovereignty – and therefore jurisdiction – is also "closely linked with the principle[ ] of . . . non-intervention," which "involves the right of every sovereign State to conduct its affairs without outside interference." *Military and Paramilitary Activities in and against Nicaragua (Nicar. v. US)*, 1986 ICJ 14, para. 202 (27 June); *see also* Oppenheim, *supra*, at 428 (stating that the principle of non-intervention "is the corollary of every state's right to sovereignty, territorial integrity and political independence.").

The scope of a state's extraterritorial jurisdictional competence depends on the type of jurisdiction exercised by the state. *Restatement (Third*), *supra*, at §401 cmt. a ("The limitations on a state's authority to subject foreign interests or activities to its laws differ from those that govern the state's jurisdiction to adjudicate, and [from] the limitations on a state's authority to enforce its law . . . ."). 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"). *Id*. at §401. In the criminal context, the U.S. exercises enforcement jurisdiction when it seeks to "effect 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. *See* SS Lotus (Fr. v. Turk.) 1927 P.C.I.J. (ser. A) No. 10, at 18-19 (Sept. 7). 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 §433(1)(a); *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, *supra*, at 18; Arrest Warrant of 11 April 2000 (Dem. Rep. Congo v. Belg.) 2002 I.C.J. 3, at paras. 4, 49, 54 (Feb. 14)). This jurisdictional constraint – *i.e.* the requirement of consent – is rooted in the principle of sovereignty for any unilateral exercise of enforcement jurisdiction on another state's territory would violate that state's sovereignty by usurping its sovereign powers. *See generally* SS Lotus, *supra*, at 18; Ian Brownlie, *Principles of Public International Law* 478-79 (8th ed. 2012); Michael Akehurst, *Jurisdiction in International Law*, 46 Brit. Y. B. Int'l L. 145, 145-151 (1975).

The territorial constraints on the exercise of enforcement jurisdiction apply to remote searches and seizures of devices located abroad. As a general matter, the principle of "State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of [information and communications technology]-related activities and to their jurisdiction over ICT infrastructure within their territory."[11] *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶25, *delivered to the General Assembly*, U.N.

[11] For that reason, "cyber activities and the individuals who engage in them are subject to the same jurisdictional prerogatives and limitations as any other form of activity." *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations* Rule 8, para. 2 (Michael N. Schmitt ed. 2017).

Doc. A/70/174 (July 22, 2015); *see also id.* para. 26(b) ("In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality . . . and non-intervention in the internal affairs of other States. Existing obligations under international law are applicable to State use of ICTs."). This principle is specifically applied to law enforcement in the digital context in the Council of Europe's Convention on Cybercrime, which was ratified by the U.S. in 2006 and promulgates "a common criminal policy aimed at the protection of society through cybercrime," including through international cooperation. Council on Europe, Convention on Cybercrime pmbl., *opened for signature* Nov. 23, 2004, S. Treaty Doc. No. 108-11 (2006), 2296 U.N.T.S. 167 (entered into force July 1, 2004); *see also* Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 Cal. L. Rev. 817, 862 (2012) (describing the Convention as "the first international treaty on crimes committed using the Internet and other computer networks"). The Convention drafters, in considering digital searches and seizures, came to "the common understanding . . . that investigative activity of law enforcement authorities of a State Party in international communication networks or in computer systems located in the territory of another state may amount to a violation of territorial sovereignty of the state concerned, and therefore cannot be undertaken without prior consent of" that state. Henrik W.K. Kaspersen, Council of Europe, *Cybercrime and Internet Jurisdiction* 26 (2009). Article 32 of the

Convention reflects this understanding by permitting "trans-border access to stored computer data" only "with consent or where publicly available."[12] Convention on Cybercrime, *supra*, art. 32; *see also* 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,

[12] An example where "data is not meant to be available" would be "if a law enforcement agency hacks into a suspected criminal's computer located in another State." *Tallinn Manual 2.0*, *supra*, at Rule 11, para. 14. In those circumstances, "it is exercising enforcement jurisdiction in that State and the activity requires the latter State's consent . . . ." *Id.*

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 4 (Sept. 18, 2013) (ER.S.VI 1087); *see also infra* note 15. 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 under Rule 41 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.[13] The NIT's extraterritorial reach was foreseeable from the government's warrant application. The government submitted that "[t]he Tor network . . . obscure[e]s a user's true location" and accordingly requested "authority to use the NIT . . . to investigate *any* user or administrator who logs into the TARGET WEBSITE. NIT Aff. ¶¶8, 32

[13] 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 4 (ER.S.VI 1087). The government therefore submits that "the search of electronic storage media located" abroad constitutes an extraterritorial search.

(ER.S.V 933, 946) (emphasis added). The warrant application further explained that the NIT would "reveal to the government . . . information that may assist in identifying the user's computer, *its location*, and the user of the computer." *Id*. at ¶34 (ER.S.V 946-47) (emphasis added); *see also id*. at ¶10 (ER.S.V 934) (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. 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=2015-02-01&end=2015-02-28 (last visited Oct. 14, 2017) (refining search of "Top-10 countries by relay users" to the month of February 2015). Moreover, in its warrant application, the government submitted that among "the sections, forums, and sub-forums" it "observed" on the Playpen website were those dedicated to "Other Languages," including Italian, Portuguese, German, Spanish, Dutch and Russian, suggesting that some portion of visitors to the site were foreign. NIT Aff. ¶14 (ER.S.V 938). The NIT warrant application therefore implicitly requested authority to conduct extraterritorial searches and seizures – and indeed those searches and seizures were carried out. Accordingly, the NIT warrant is invalid because the magistrate judge lacked authority under Rule 41 to issue a warrant authorizing 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, under well-established principles of international law, the unilateral exercise of extraterritorial enforcement jurisdiction may constitute a violation of sovereignty. *See supra* 14-18. 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 Computers and Obtaining Electronic Evidence in Criminal Investigations* 85 (2009).

Consent helps avoid jurisdictional – and thereby diplomatic – conflict between states.[14] The U.S. traditionally relies on consent-based mechanisms for obtaining evidence located extraterritorially. The principal mechanism is a Mutual Legal Assistance Treaty ("MLAT"), a bilateral agreement containing procedures for obtaining and providing assistance in criminal matters.[15] *See* T. Markus Funk, Fed. Judicial Ctr., *Mutual Legal Assistance Treaties and Letters Rogatory: A Guide for Judges* 5 (2014). The U.S. is also party to a number of multilateral treaties that similarly provide a basis for obtaining and providing assistance in criminal matters among a broader group of countries.[16] *See e.g.*, Convention on

[14] 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).

[15] 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.

[16] Law enforcement agencies may also participate directly in various other types of cooperative arrangements. The U.S. is, for example, a member of the International

Cybercrime, *supra; see generally*, Dep't of Justice, Office of International Affairs, https://www.justice.gov/criminal-oia (last visited Oct. 14, 2017) (describing OIA as "employ[ing] a vast network of international relationships and treaties to obtain essential evidence located abroad . . . and secure other assistance necessary for successful U.S. criminal investigations and prosecutions"). Here, however, the government unilaterally deployed the NIT, without seeking consent through one of these existing mechanisms. *See* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 Stan. L. Rev. 1075, 1118 (2017) ("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.).

The government's deployment of the NIT poses particular risks. 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,

Criminal Police Organization (Interpol), which enables countries to route requests for law enforcement assistance through its network. Michael Abbell, *Obtaining Evidence Abroad in Criminal Cases* 9 & n.47 (2010). 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.

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. Was the purpose of the hack to conduct surveillance, steal information, or interfere with political institutions? It may also be difficult to identify the actor behind the attack. Was it another state, hackers affiliated with that state, or a group of criminals? These uncertainties can potentially heighten the risk of diplomatic conflict. *See Report of the Group of Governmental Experts*, *supra*, at paras 16(b), 17 (noting "the risk of misperception, escalation and conflict that may stem from ICT incidents" and recommending enhanced international cooperation with respect to law enforcement investigations).

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.[17] *See supra* 22. Reversing the scenario, foreign deployment of a NIT-like technique

[17] It may also interfere with active criminal investigations by the other countries' authorities.

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.[18] Brunker, *supra*; *see also United States v. Gorshkov*, No. 00-cr-550, 2001 WL 1024026 (W.D. Wash., May 23, 2001).

Finally, it is worth considering whether the authorization of the NIT warrant – in defiance of well-established international law – will encourage other countries to engage in similar conduct. By asserting an exception to the prohibition against unilateral extraterritorial searches and seizures, the U.S. runs the risk that other

[18] 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").

countries may claim such an exception for themselves. Would another country's unilateral use of a NIT or similar technique against the devices of Americans – even for law enforcement purposes – be acceptable to the government? Or would the government consider such action to constitute a violation of American sovereignty? As these questions and the discussion above illustrate, the NIT's extraterritorial reach raises complex foreign relations considerations, further counselling against authorization of the NIT warrant.

CONCLUSION

For the reasons set forth above, *amicus curiae* Privacy International respectfully submits that the NIT's extraterritorial reach renders the warrant invalid and therefore requests that this Court reverse the district court's denial of Mr. Tippens's motions to suppress.

Dated October 20, 2017

Respectfully submitted,

/s/ Scarlet Kim
Scarlet Kim
Counsel for Amicus Curiae

Privacy International
62 Britton Street
London EC1M 5UY
+44 (0) 20 3422 4321
scarlet@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 6,156 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). Circuit Rule 32-1(a) provides that "[t]he opening and answering briefs filed by appellant and appellee, respectively, may not exceed 14,000 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.* 7,000 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 October 20, 2017

/s/ Scarlet Kim
Scarlet Kim
Counsel for Amicus Curiae

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

CERTIFICATE OF SERVICE

I certify that on October 20, 2017, I filed the Brief of Amicus Curiae Privacy International with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system. Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

Dated October 20, 2017

/s/ Scarlet Kim
Scarlet Kim
Counsel for Amicus Curiae

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