



**U.S. Department of Justice**

Criminal Division

---

Office of Enforcement Operations

Washington, D.C. 20530

**VIA Electronic Mail**

February 19, 2020

Jonathan Manes, Esq.  
Civil Liberties and Transparency Clinic  
University at Buffalo School of Law  
507 O'Brian Hall, North Campus  
Buffalo, NY 14260  
[jmmanes@buffalo.edu](mailto:jmmanes@buffalo.edu)

Request No. CRM-300680988  
Privacy International et al., v. Federal Bureau  
of Investigation, et al., 18-cv-1488  
(W.D.N.Y.)

Dear Mr. Manes:

This is the third installment of the Criminal Division's rolling production regarding your Freedom of Information Act request dated September 10, 2018, for certain records pertaining to "computer network exploitation" or "network investigative techniques." Your request is currently in litigation, Privacy International, et al. v. Federal Bureau of Investigation, et al., 18-cv-1488 (W.D.N.Y.). You should refer to this case number in any future correspondence with this Office. This request is being processed in accordance with the interpretation and parameters set forth by defendants in the July 12, 2019, letter to you from Senior Trial Counsel Marcia Sowles, as well as subsequent conversations regarding the Criminal Division's processing of the request.

Please be advised that a search has been conducted in the appropriate sections, and we are continuing to review and process potentially responsive records. After carefully reviewing 521 pages of records, I have determined that 436 pages are responsive to your request: 380 pages are appropriate for release in full, copies of which are enclosed. Additionally, seven pages are appropriate for release in part and forty-nine pages are exempt from disclosure pursuant to:

5 U.S.C. § 552(b)(5), which concerns certain inter- and intra-agency communications protected by the deliberative process privilege, the attorney work-product privilege, and the attorney-client privilege;

5 U.S.C. § 552(b)(6), which concerns material the release of which would constitute a clearly unwarranted invasion of the personal privacy of third parties;

5 U.S.C. § 552(b)(7)(C), which concerns records or information compiled for law enforcement purposes the release of which could reasonably be expected to constitute an unwarranted invasion of the personal privacy of third parties; and

5 U.S.C. § 552(b)(7)(E), which concerns records or information compiled for law enforcement purposes the release of which would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law

enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law.

For your information, Congress excluded three discrete categories of law enforcement and national security records from the requirements of the FOIA. See 5 U.S.C. § 552(c). This response is limited to those records that are subject to the requirements of the FOIA. This is a standard notification that is given to all our requesters and should not be taken as an indication that excluded records do, or do not, exist.

You may contact Senior Trial Counsel Marcia K. Sowles by phone at (202) 514-4960, by email at [Marcia.Sowles@usdoj.gov](mailto:Marcia.Sowles@usdoj.gov), or by mail at the Civil Division, Federal Programs Branch, 1100 L Street, N.W., Room 10028, Washington, D.C. 20005, for any further assistance and to discuss any aspect of your request.

Although I am aware that your request is the subject of ongoing litigation and that appeals are not ordinarily acted on in such situations, I am required by statute and regulation to inform you of your right to an administrative appeal of this determination. If you are not satisfied with my response to this request, you may administratively appeal by writing to the Director, Office of Information Policy (OIP), United States Department of Justice, 441 G Street, NW, 6th Floor, Washington, D.C. 20530, or you may submit an appeal through OIP's FOIA STAR portal by creating an account on the following website: <https://foiastar.doj.gov>. Your appeal must be postmarked or electronically transmitted within 90 days of the date of my response to your request. If you submit your appeal by mail, both the letter and the envelope should be clearly marked "Freedom of Information Act Appeal."

Sincerely,



Amanda Marchand Jones  
Chief  
FOIA/PA Unit

cc: Marcia K. Sowles  
Senior Trial Counsel  
Civil Division, Federal Programs Branch  
1100 L Street, N.W., Room 11028  
Washington, D.C. 20005  
[Marcia.Sowles@usdoj.gov](mailto:Marcia.Sowles@usdoj.gov)

Michael S. Cerrone  
[michael.cerrone@usdoj.gov](mailto:michael.cerrone@usdoj.gov)

Enclosures

# Rule 41 and Remote Searches

---

Erica O'Neil, Asst. Deputy Chief, CCIPS

(b) (6), (b) (7)(C)@usdoj.gov

# Framework

---

- Rule 41(b)(6) and venue for search warrants
- Using remote searches in your dark market cases
- Rule 41(b)(6) issues and pitfalls

# Venue for Search Warrants

---

# Venue

---

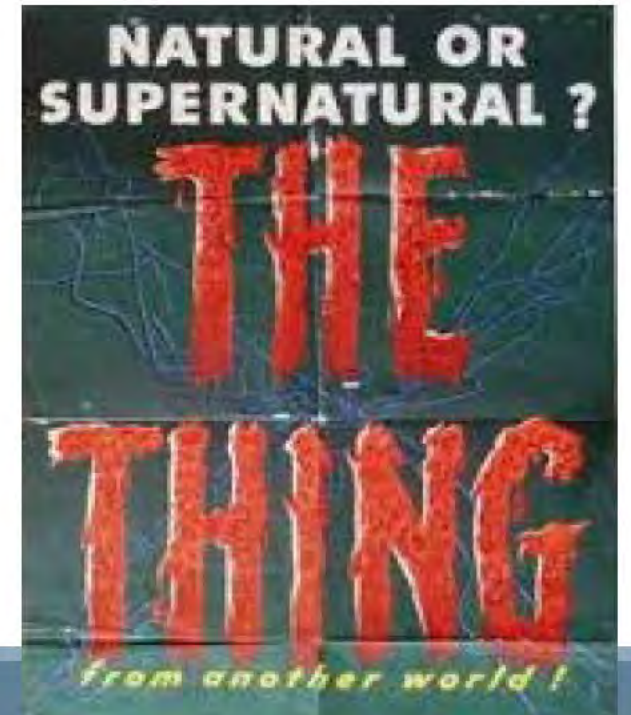
- Traditional (physical) searches
- Venue is easy
- Where is property to be searched located?
  - Apply for your warrant there



# SCA Warrants

---

- (b) (5)
- Venue is based on “court of competent jurisdiction”
  - is in district where provider is located or
  - has jurisdiction over the offense being investigated;
- 18 U.S.C. § 2711(3)(A)



# And the newest addition:

---

- Rule 41(b)(6)
- Remote searches of computers if:
  - (A) Concealed by technological means or
  - (B) Botnets





# Rule 41(b)(6)(A)

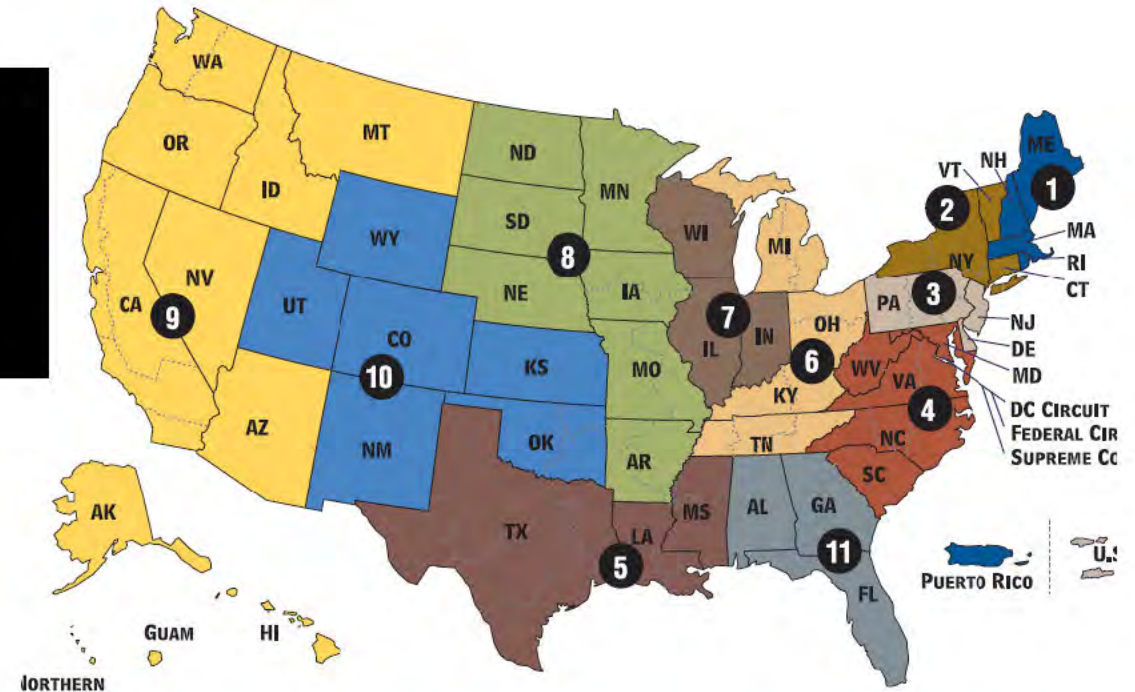
---

- a magistrate judge with authority in any district where activities related to a crime may have occurred
- has authority 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;

# Venue – where to apply

- In any district where activities related to a crime may have occurred

➤ (b) (5)



# Authority

---

- a magistrate judge has authority to issue a warrant to use **remote access to search** electronic storage media



# Location of Data

---

- and to seize or copy electronically stored information **located within or outside that district**



# Concealment

---

- If the district where the media or information is located has been concealed through technological means;



# Uses

---

# Locating Your Target

---

- NIT sent to target through document
- Usually to obtain true IP address

**(b) (7)(E)**

# Building A Tool

---

- How creative are the agents & computer scientists in your district?





# Issues and Pitfalls

---

# Questions?

---

(b) (6), (b) (7)(C) @usdoj.gov

(b) (6), (b) (7)(C)

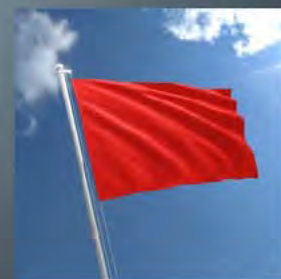
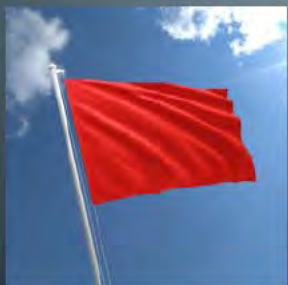
## REMOTE SEARCHES

- Rule 41(B)(6): a court where activities relating to a crime may have occurred can issue warrant for remote search if:
  - (A) location of computer has been concealed through technological means (i.e. proxy); or
  - (B) victim computers of 1030(a)(5)(A) located in 5 or more districts

- Otherwise:



## FOREIGN EVIDENCE: REMOTE SEARCHES



# Obtaining the Warrant: Jurisdiction

- Rule 41(b) governs the jurisdiction of courts to issue warrants
- Common question: where does jurisdiction lie to authorize a remote search?
  - Rule 41(b)(6) provides jurisdiction for issuing warrant for remote searches in limited circumstances
  - Litigation risk exists in other circumstances

# REMOTE SEARCHES

- Rule 41(b)(6): location of computer concealed via technological means (i.e. TOR/proxy)

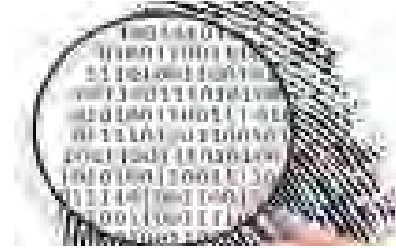
- Otherwise:



## NITs Make Nice: Defeating an Offender's Use of Proxies by Employing a Network Investigative Technique (NIT)

By (b)(6), (7)(C) CEOS Trial Attorney

Sophisticated online offenders have increasingly turned to anonymization technologies, such as proxy servers, to hide their true location and identity from law enforcement. See CEOS Quarterly Newsletter (September 2009), *Proxies, Anonymizers, Private Networks and You: A Primer on Internet Misdirection, Deception, and Finger Pointing*. Law enforcement is not, however, without techniques to defeat anonymization. One option is a Network Investigative Technique, or "NIT." This article discusses the use of one type of NIT and the process required to obtain authorization for it.

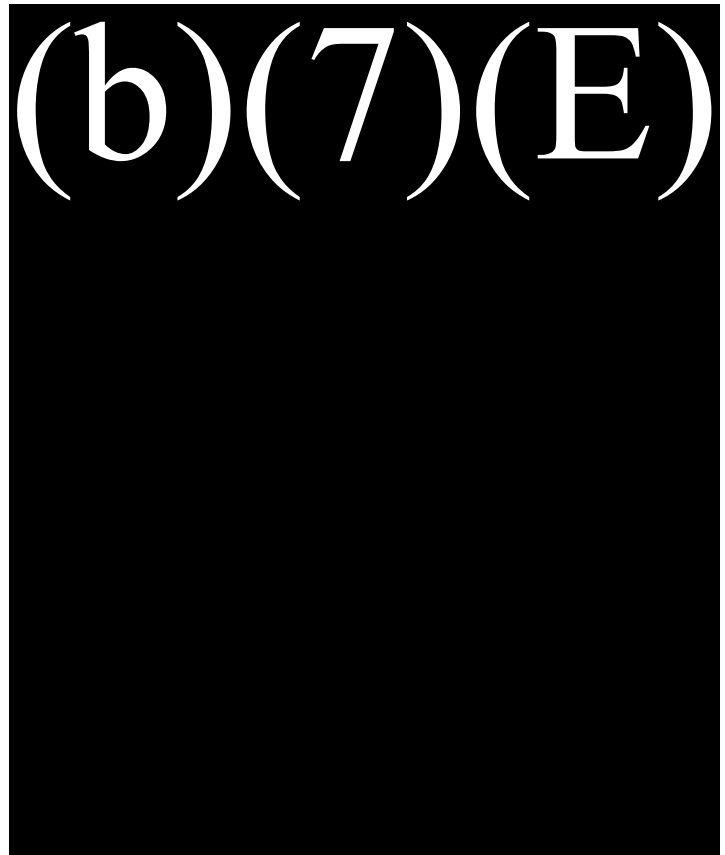


### I. What is a NIT?

A NIT is a tool that allows law enforcement to remotely collect information from a target computer. Computer code is delivered to the target computer; the code runs or activates on the target computer; and that information is delivered to a government-controlled computer.

### II. How Does a NIT Work?

The exact specifications and design of a NIT will vary based upon your forensic agent or programmer and the information you are seeking.



### IV. What Sort of Information Can a NIT Collect?

In the context of an offender who is using a proxy server, the primary objective of a NIT is to identify the actual IP address of the offender. However, a NIT can obtain other useful -- and potentially identifying -- information as well. For example, a

(b)(7)(E)

(b)(7)(E)

V. What Authorization is Needed to Implement a NIT?

As with many issues involving electronic evidence, technology advances faster than the law. (b)(5)

(b)(5)

(b)(5)

(b)(5), (7)(E)

(b)(5)

VII. Conclusion

A NIT can be a creative technological solution to the difficult and increasingly prevalent problem of anonymization use by offenders. By measures such as causing offenders' true IP addresses to be sent to the government, NITs can help law enforcement identify those who believe they are able to commit child exploitation crimes free of the risk of being caught. ▣



**UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF TEXAS  
HOUSTON DIVISION**

IN RE WARRANT TO SEARCH A TARGET §  
COMPUTER AT PREMISES UNKNOWN § CASE NO. H-13-234M  
§  
§

**MEMORANDUM AND ORDER**

The Government has applied for a Rule 41 search and seizure warrant targeting a computer allegedly used to violate federal bank fraud, identity theft, and computer security laws. Unknown persons are said to have committed these crimes using a particular email account via an unknown computer at an unknown location. The search would be accomplished by surreptitiously installing software designed not only to extract certain stored electronic records but also to generate user photographs and location information over a 30 day period. In other words, the Government seeks a warrant to hack a computer suspected of criminal use. For various reasons explained below, the application is denied.

**Background**

In early 2013, unidentified persons gained unauthorized access to the personal email account of John Doe, an individual residing within the Southern District of Texas, and used that email address to access his local bank account. The Internet Protocol (IP) address of the computer accessing Doe's account resolves to a foreign country. After Doe discovered the breach and took steps to secure his email account, another email account nearly identical to Doe's the address differed by a single letter was used to attempt a sizeable wire

transfer from Doe's local bank to a foreign bank account. The FBI has commenced an investigation, leading to this search warrant request. At this point in the investigation, the location of the suspects and their computer is unknown.

The Government does not seek a garden-variety search warrant. Its application requests authorization to surreptitiously install data extraction software on the Target Computer. Once installed, the software has the capacity to search the computer's hard drive, random access memory, and other storage media; to activate the computer's built-in camera; to generate latitude and longitude coordinates for the computer's location; and to transmit the extracted data to FBI agents within this district.

Using this software, the government seeks to obtain the following information:

(1) records existing on the Target Computer at the time the software is installed, including:

- records of Internet Protocol addresses used;
- records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" Web pages, search terms that the user entered into any Internet search engine, and records of user-typed Web addresses;
- records evidencing the use of the Internet Protocol addresses to communicate with the [victim's bank's] e-mail servers;
- evidence of who used, owned, or controlled the TARGET COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs registry entries, configuration file, saved user names and passwords, documents, browsing history, user profiles, e-mail contents, e-mail contacts, "chat," messaging logs, photographs, and correspondence;
- evidence of software that would allow others to control the TARGET

COMPUTER;

- evidence of times the TARGET COMPUTER was used; and
- records of applications run.

(2) prospective data obtained during a 30-day monitoring period, including:

- accounting entries reflecting the identification of new fraud victims;
- photographs (with no audio) taken using the TARGET COMPUTER's built-in camera after the installation of the NEW SOFTWARE, sufficient to identify the location of the TARGET COMPUTER and identify persons using the TARGET COMPUTER;
- information about the TARGET COMPUTER's physical location, including latitude and longitude calculations the NEW SOFTWARE causes the TARGET COMPUTER to make;
- records of applications run.

Aff. Attach. B.<sup>1</sup>

### **Analysis**

The Government contends that its novel request<sup>2</sup> is authorized by Rule 41. In the

---

<sup>1</sup> At the Government's request, the warrant application has been sealed to avoid jeopardizing the ongoing investigation. This opinion will not be sealed because it deals with a question of law at a level of generality which could not impair the investigation.

<sup>2</sup> This appears to be a matter of first impression in this (or any other) circuit. The Court has found no published opinion dealing with such an application, although in 2007 a magistrate judge is known to have issued a warrant authorizing a similar investigative technique to track the source of e-mailed bomb threats against a Washington state high school. *See* Application and Affidavit for Search Warrant, In the Matter of the Search of Any Computer Accessing Electronic Message(s) Directed to Administrator(s) of MySpace Account "Timberlinebombinfo" and Opening Messages Delivered to That Account by the Government at 2, No. MJ07-5114 (W. D. Wash. June 12, 2007), available at <http://www.politechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf>.

Court's view, this claim raises a number of questions, including: (1) whether the territorial limits of a Rule 41 search warrant are satisfied; (2) whether the particularity requirements of the Fourth Amendment have been met; and (3) whether the Fourth Amendment requirements for video camera surveillance have been shown. Each issue is discussed in turn.

**1. Rule 41(b) Territorial Limit**

Rule 41(b) sets out five alternative territorial limits on a magistrate judge's authority to issue a warrant. The government's application does not satisfy any of them.

The rule's first subsection, the only one expressly invoked by the Government's application, allows a "magistrate judge with authority in the district . . . to issue a warrant to search for and seize a person or property located within the district." FED. R. CRIM. P. 41(b)(1). Even though the Government readily admits that the current location of the Target Computer is unknown, it asserts that this subsection authorizes the warrant "because information obtained from the Target Computer will first be examined in this judicial district." Aff. ¶ 20. Under the Government's theory, because its agents need not leave the district to obtain and view the information gathered from the Target Computer, the information effectively becomes "property located within the district." This rationale does not withstand scrutiny.

It is true that Rule 41(a)(2)(A) defines "property" to include "information," and the Supreme Court has long held that "property" under Rule 41 includes intangible property such as computer data. *See United States v. New York Tel. Co.*, 434 U.S. 159, 170 (1977). For

purposes of search and seizure law, many courts have analogized computers to large containers filled with information.<sup>3</sup> See *United States v. Roberts*, 86 F. Supp. 2d 678, 688 (S.D. Tex. 2000); *United States v. Barth*, 26 F. Supp. 2d. 929, 936-37 (W.D. Tex. 1998); *United States v. David*, 756 F. Supp. 1385, 1390 ( D. Nev. 2009) (holding that a computer notebook “is indistinguishable from any other closed container” for the purpose of Fourth Amendment analysis). By the Government’s logic, a Rule 41 warrant would permit FBI agents to roam the world in search of a container of contraband, so long as the container is not opened until the agents haul it off to the issuing district. The court has found no case willing to stretch the territorial limits of Rule 41(b)(1) so far.

The “search” for which the Government seeks authorization is actually two-fold: (1) a search for the Target Computer itself, and (2) a search for digital information stored on (or generated by) that computer. Neither search will take place within this district, so far as the Government’s application shows. Contrary to the current metaphor often used by Internet-based service providers, digital information is not actually stored in clouds; it resides on a computer or some other form of electronic media that has a physical location.<sup>4</sup> Before that digital information can be accessed by the Government’s computers in this district, a search

---

<sup>3</sup> Some scholars have challenged the aptness of the container metaphor, noting that the ever-growing storage capacity of an ordinary hard drive more closely resembles a library than a filing cabinet. See Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 Virginia Law Review In Brief 1, 5-6 (2011).

<sup>4</sup> See generally H. Marshall Jarrett et al., *U.S. Dep’t of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* 84-85 (2009), available at <http://www.justice.gov/criminal/cybercrime/docs/ssmanual2009.pdf>.

of the Target Computer must be made. That search takes place, not in the airy nothing of cyberspace, but in physical space with a local habitation and a name. Since the current location of the Target Computer is unknown, it necessarily follows that the current location of the information on the Target Computer is also unknown. This means that the Government's application cannot satisfy the territorial limits of Rule 41(b)(1).

This interpretation of (b)(1) is bolstered by comparison to the territorial limit of subsection (b)(2), which expressly deals with a transient target. This subsection allows an extraterritorial search or seizure of moveable property "if it is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed." FED. R. CRIM. P. 41(b)(2). Note that (b)(2) does not authorize a warrant in the converse situation that is, for property *outside* the district when the warrant is issued, but brought back *inside* the district before the warrant is executed. A moment's reflection reveals why this is so. If such warrants were allowed, there would effectively be no territorial limit for warrants involving personal property, because such property is moveable and can always be transported to the issuing district, regardless of where it might initially be found.<sup>5</sup>

---

<sup>5</sup> This situation should be distinguished from an anticipatory warrant, which may be issued upon a showing of (1) a fair probability that contraband or evidence of a crime will be found in a particular place if a triggering condition occurs, and (2) probable cause to believe the triggering condition will occur. *United States v. Grubbs*, 547 U.S. 90, 96-97 (2006). Here the "triggering condition" is the installation of software which will "extract" (i.e. seize) the computer data and transmit it to this district. This "triggering condition" is itself a search or seizure that separately requires a warrant.

The other subsections of Rule 41(b) likewise offer no support for the Government's application. Subsection (b)(3), dealing with an investigation of domestic or international terrorism, authorizes a search by a magistrate judge with authority in "any district in which activities related to the terrorism may have occurred," whether the property is within or outside that district. This case does not involve a terrorism investigation.

Subsection (b)(4) deals with a tracking device warrant, and its provisions echo those of (b)(2), allowing the device to be monitored outside the district, provided the device is installed within the district. FED. R. CRIM. P. 41(b)(4). There is a plausible argument that the installation of software contemplated here falls within the statutory definition of a tracking device,<sup>6</sup> because the software will activate the computer's camera over a period of time and capture latitude/longitude coordinates of the computer's physical location. But the Government's application would fail nevertheless, because there is no showing that the installation of the "tracking device" (i.e. the software) would take place within this district. To the contrary, the software would be installed on a computer whose location could be anywhere on the planet.<sup>7</sup>

The only remaining possibility is (b)(5), which authorizes a magistrate judge "in any district where activities related to the crime may have occurred" to issue a warrant for

---

<sup>6</sup> See 18 U.S.C. § 3117(b) ("an electronic or mechanical device which permits the tracking of the movement of a person or object").

<sup>7</sup> According to the Government's application, the Target Computer's last known internet protocol address resolved to a country in Southeast Asia.

property that may be outside the jurisdiction of any state or district, but within a U.S. territory, possession, commonwealth, or premises used by a U.S. diplomatic or consular mission. FED. R. CRIM. P. 41(b)(5). The application does indicate that Doe's local bank account was improperly accessed, thereby satisfying (b)(5)'s initial condition. However, the remaining territorial hurdle of this subsection is not satisfied, because there is no evidence the Target Computer will be found on U.S.-controlled territory or premises.

## **2. Fourth Amendment particularity requirement**

The Fourth Amendment prescribes that “no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and *particularly describing the place to be searched, and the persons or things to be seized.*” This particularity requirement arose out of the Founders' experience with abusive general warrants. *See Steagald v. United States*, 451 U.S. 204, 220 (1981); *see generally* William J. Cuddihy, *The Fourth Amendment: Origins and Original Meaning* 602-1791 (2009).

As previously noted, the warrant sought here would authorize two different searches: a search *for* the computer used as an instrumentality of crime, and a search *of* that computer for evidence of criminal activity. Because the latter search presumes the success of the initial search for the Target Computer, it is appropriate to begin the particularity inquiry with that initial search.

The Government's application contains little or no explanation of how the Target Computer will be found. Presumably, the Government would contact the Target Computer



via the counterfeit email address, on the assumption that only the actual culprits would have access to that email account. Even if this assumption proved correct, it would not necessarily mean that the government has made contact with the end-point Target Computer at which the culprits are sitting. It is not unusual for those engaged in illegal computer activity to “spoof” Internet Protocol addresses as a way of disguising their actual on-line presence; in such a case the Government’s search might be routed through one or more “innocent” computers on its way to the Target Computer.<sup>8</sup> The Government’s application offers nothing but indirect and conclusory assurance that its search technique will avoid infecting innocent computers or devices:

Further, the method in which the software is added to the TARGET COMPUTER is designed to ensure that the [persons] committing the illegal activity will be the only individuals subject to said technology.

Aff. ¶ 17.<sup>9</sup> This “method” of software installation is nowhere explained.<sup>10</sup> Nor does the Government explain how it will ensure that only those “committing the illegal activity will

---

<sup>8</sup> See Neal K. Katyal, *Criminal Law in Cyberspace*, 149 U. Pa. L. Rev. 1003, 1028 (2001).

<sup>9</sup> The quoted passage is from the revised affidavit submitted by the FBI agent in response to the court’s expressed concerns about the lack of particularity in the initial affidavit.

<sup>10</sup> In response to a FOIA request several years ago, the FBI publicly released information about a Web-based surveillance tool called “Computer and Internet Protocol Address Verifier” (CIPAV). See <https://www.eff.org/deeplinks/2011/04/new-fbi-documents-show-depth-government> . Although apparently in routine use as a law enforcement tool, the court has found no reported case discussing CIPAV in the context of a Rule 41 search warrant (or any other context, for that matter).

be . . . subject to the technology.” What if the Target Computer is located in a public library, an Internet café, or a workplace accessible to others? What if the computer is used by family or friends uninvolved in the illegal scheme? What if the counterfeit email address is used for legitimate reasons by others unconnected to the criminal conspiracy? What if the email address is accessed by more than one computer, or by a cell phone and other digital devices? There may well be sufficient answers to these questions, but the Government’s application does not supply them.

The court concludes that the revised supporting affidavit does not satisfy the Fourth Amendment’s particularity requirement for the requested search warrant for the Target Computer.

### **3. Constitutional standards for video camera surveillance**

As explained above, the Government’s data extraction software will activate the Target Computer’s built-in-camera and snap photographs sufficient to identify the persons using the computer. The Government couches its description of this technique in terms of “photo monitoring,” as opposed to video surveillance, but this is a distinction without a difference. In between snapping photographs, the Government will have real time access to the camera’s video feed. That access amounts to video surveillance.

The Fifth Circuit has described video surveillance as “a potentially indiscriminate and most intrusive method of surveillance.” *United States v. Cuevas-Sanchez*, 821 F.2d 248, 250 (5th Cir. 1987). In that case the court adopted constitutional standards for such surveillance

by borrowing from the statute permitting wiretaps Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S. C. §§ 2510-2520. *Id.*, citing *United States v. Biasucci*, 786 F.2d 504 (2nd Cir.), *cert. denied*, 479 U.S. 827 (1986). Under those standards, a search warrant authorizing video surveillance must demonstrate not only probable cause to believe that evidence of a crime will be captured, but also should include: (1) a factual statement that alternative investigative methods have been tried and failed or reasonably appear to be unlikely to succeed if tried or would be too dangerous; (2) a particular description of the type of communication sought to be intercepted, and a statement of the particular offense to which it relates; (3) a statement of the duration of the order, which shall not be longer than is necessary to achieve the objective of the authorization nor, in any event, longer than 30 days, (though extensions are possible); and (4) a statement of the steps to be taken to assure that the surveillance will be minimized to effectuate only the purposes for which the order is issued. *Cuevas-Sanchez*, 821 F.2d at 252.

The Government's application fails to meet the first and fourth of these criteria, *i.e.* inadequate alternatives and minimization. Regarding the inadequacy of alternative investigative techniques, the Government offers only a conclusory statement:

Investigative methods that might be alternatives to the use of a camera attached to the TARGET COMPUTER reasonably appear to be unlikely to succeed if tried or would be too dangerous.

Aff. ¶ 14. The Government makes no attempt to explain why this is so. In fact, contemporaneous with this warrant application, the Government also sought and obtained

an order under 18 U.S.C. § 2703 directing the Internet service provider to turn over all records related to the counterfeit email account, including the contents of stored communications. To support that application, an FBI agent swore that the ISP's records would likely reveal information about the "identities and whereabouts" of the users of this account. Yet the same agent now swears that no other technique is likely to succeed. The Government cannot have it both ways. *See Cuevas-Sanchez*, 821 F.2d at 250 (" A juxtaposition of such contentions trifles with the Court.") (citation omitted).

As for minimization, the Government has offered little more than vague assurances:

Steps will be taken to assure that data gathered through the technique will be minimized to effectuate only the purposes for which the warrant is issued. The software is not designed to search for, capture, relay, or distribute personal information or a broad scope of data. The software is designed to capture limited amounts of data, the minimal necessary information to identify the location of the TARGET COMPUTER and the user of TARGET COMPUTER.

Aff. ¶ 17. The steps taken to minimize over-collection of data are left to the court's imagination. The statement that the software is designed to capture only limited amounts of data "the minimal necessary information needed to identify the location of the Target Computer and the user" does mitigate the risk of a general search somewhat, but that assurance is fatally undermined by the breadth of data authorized for extraction in the proposed warrant. *See* Aff. Attach. B, described *supra* at p. 2-3. Software that can retrieve this volume of information Internet browser history, search terms, e-mail contents and contacts, "chat", instant messaging logs, photographs, correspondence, and records of


applications run, among other things is not fairly described as capturing “only limited amounts of data.” Finally, given the unsupported assertion that the software will not be installed on “innocent” computers or devices, there remains a non-trivial possibility that the remote camera surveillance may well transmit images of persons not involved in the illegal activity under investigation.

For these reasons, the Government has not satisfied the Fourth Amendment warrant standards for video surveillance.

### **Conclusion**

The court finds that the Government’s warrant request is not supported by the application presented. This is not to say that such a potent investigative technique could never be authorized under Rule 41. And there may well be a good reason to update the territorial limits of that rule in light of advancing computer search technology. But the extremely intrusive nature of such a search requires careful adherence to the strictures of Rule 41 as currently written, not to mention the binding Fourth Amendment precedent for video surveillance in this circuit. For these reasons, the requested search and seizure warrant is denied.

Signed at Houston, Texas on April 22, 2013.

  
Stephen Wm Smith  
United States Magistrate Judge

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

<b>UNITED STATES OF AMERICA,</b>	)	
	)	
<b>Plaintiff,</b>	)	
	)	
<b>v.</b>	)	<b>Case No. 15-CR-182-JHP</b>
	)	
<b>SCOTT FREDRICK ARTERBURY,</b>	)	
	)	
<b>Defendant.</b>	)	

**REPORT AND RECOMMENDATION**

Before the Court is the Motion to Suppress Evidence Seized from Residence (“Motion to Suppress”) and Request for an Evidentiary Hearing of Defendant Scott Fredrick Arterbury (“Arterbury”). [Dkt. No. 33]. On March 23, 2016, the matter was referred to the undersigned United States Magistrate Judge for Report and Recommendation on the Motion to Suppress. [Dkt. No. 35]. The Motion for hearing has been **GRANTED**, and a hearing conducted on April 25, 2016. After considering the submissions of the parties and the arguments of counsel, the undersigned makes the following findings and recommendation to the District Court.

**I.  
FACTUAL BACKGROUND – THE “DARK NET” OR TOR**

This case involves what is known as the “The Dark Net,” the “Tor Network” or “Tor” for short.<sup>1</sup> “Tor is an open-source tool that aims to provide

---

<sup>1</sup> The Dark Net generally refers to “an area of the Internet only accessible by using an encryption tool called The Onion Router (Tor). Tor is a tool aimed at those desiring privacy online, although frequently attracting those with criminal intentions.” Gareth Owen and Nick Savage, “The Tor Dark Net”, at 1

anonymity and privacy to those using the Internet. It prevents someone who is observing the user from identifying which sites they are visiting and it prevents sites from identifying the user. Some users value Tor's anonymity because it makes it difficult for governments to censor sites or content that may be hosted elsewhere in the world." Owen and Savage, at 1. An individual living under a repressive government such as North Korea, for example, might make use of Tor to access or post certain information while avoiding government surveillance. However, after analyzing Tor Dark net sites over a six-month period, Owen and Savage found that "the majority of sites were criminally oriented, with drug marketplaces featuring prominently. Notably, however, it was found that sites hosting child abuse imagery were the most frequently requested." *Id.*

The Tor network is designed to route communications through multiple computers, protecting the confidentiality of Internet Protocol ("IP") addresses and other identifying information. See, Keith D. Watson, *The Tor Network: A Global Inquiry into the Legal Status of Anonymity Networks*, 11 Wash. U. Global Stud. L. Rev. 715 (2012) (hereafter, "Watson"). See, for example, *U.S. v. Frater*, 2016 WL 795839, \*3 (D. Ariz. March 1, 2016).

Tor allows users to send data over the Internet anonymously by shielding the source's location. This is accomplished by a complex encryption network that dissociates Internet communication from its source's IP address. Tor achieves user anonymity through so-called "onion routing," which bounces all communications routed through the Tor network to various different "nodes" before delivering them to their destination. These "nodes" are proxy

---

[Centre for International Governance Innovation and Royal Institute of International Affairs, September 2015) (hereafter, "Owen & Savage").

servers scattered across the globe. Tor users connect to the network by first pulling in a list of nodes from a directory server. The user's computer then accesses the Tor network through a random node. The user's information is then routed through a random series of relay nodes before finally routing to an exit node, which sends the user's information to the actual Internet. What is significant about the Tor network is that each node communicates only with the nodes immediately preceding and following it in the chain. Therefore, the user's computer has direct contact with only the first node in the chain, and the actual Internet communicates only with the exit node. The entry node does not know the ultimate destination of the data, and the exit node is unaware of the data's origin. Because exit nodes are the only nodes that communicate directly with the public Internet, any traffic routed through the Tor network is traceable only to the exit node. Each communication is encrypted in a new layer of code before passing to the next node. The communication is eventually ensconced in several layers of code, which are then "peeled away" by the exit node, hence the onion metaphor.

Thus, Computer A submits data through the Tor network, the communication will pass through the network and exit onto the actual Internet through the exit node, Computer B. Any data sent by Computer A will appear to anyone tracing the communication as if it has come from Computer B. This essentially allows the user of Computer A to surf the Internet with complete anonymity, assuming the user never submits any information that is linked to her identity, such as accessing her standard e-mail account.

Watson, at 721-23.

To combat illegal activity using the Tor network, the Government has developed so-called "Trojan horse devices." These may include: "data extraction software, network investigative technique, port reader, harvesting program, remote search, CIPAV for Computer and Internet Protocol Address Verifier, or IPAV for Internet Protocol Address Verifier." Brian L. Owsley, *Beware of Government Agents Bearing Trojan Horses*, 48 Akron L. Rev. 315, 316 (2015). In the instant case, the parties have referred to the warrant issued by the U.S. magistrate judge in the Eastern District of Virginia as a Network



Investigative Technique (“NIT”) warrant, and the Court will adopt that terminology.

Once approved, the NIT is installed on the target Website. “Once installed on Website A, each time a user accessed any page of Website A, the NIT sent one or more communications to the user's computer which caused the receiving computer to deliver data to a computer controlled by the FBI, which would help identify the computer which was accessing Website A.” *U.S. v. Pierce*, 2014 WL 5173035, \*3 (D.Neb. Oct. 14, 2014). In some cases, the Government has even activated a target computer’s built-in camera to take photographs of the persons using that computer and send the photos back to the Government. *E.g., In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 759 (S.D. Tex. 2013).

The critical point is that without the use of such techniques as NIT, agents seeking to track a Tor user to his home computer will not be able to take that pursuit beyond the exit node from which the Tor user accessed the regular Internet.<sup>2</sup> NIT allows the Government to surreptitiously send a message back through the Tor network to the home computer directing it to provide information from which the user may be identified.

---

<sup>2</sup> See for example, the Affidavit of Douglas Macfarlane offered in support of the Warrant Application in the Eastern District of Virginia. [Dkt. No. 34-1]. Macfarlane states that because of the Tor Network, “traditional IP identification techniques are not viable.” [*Id.*, at ¶ 8]. “An exit node is the last computer through which a user’s communications were routed. There is no practical way to trace the user’s actual IP back through that Tor exit node IP.” [*Id.*].

## II. FACTUAL BACKGROUND OF THIS CASE

The Government obtained evidence regarding Arterbury's alleged criminal conduct through a multi-step process that began in the Fall of 2014. At that time, Agents of the Federal Bureau of Investigation ("FBI") began investigating the Playpen website, a global online forum believed to be hosting users for purposes of distributing and accessing child pornography.<sup>3</sup> In February 2015, agents apprehended the administrator of Playpen in Naples, Fla., took control of the site, and moved it to Virginia. Rather than shut Playpen down immediately, agents decided to allow the site to continue operation for 12 days (February 20, 2015 to March 4, 2015) in the hopes of identifying and prosecuting Playpen users. In furtherance of the investigation, the Government sought to use a Network Investigative Technique that would covertly transmit computer code to Playpen users. That code would direct users' computers to provide investigators with information which could then be used to locate and identify the users. In order to employ the NIT, however, the Government needed to obtain an "NIT search warrant."

In February 2015, a warrant application was prepared and presented to a magistrate judge in the Eastern District of Virginia. Absent the use of the NIT, the Government had no ability to locate and identify users of the Playpen

---

<sup>3</sup> In affidavits in support for the NIT warrant at issue, as well as various pleadings, the parties refer to "Website A." It is now widely known that Website A refers to the "Playpen," a website offering those who access it the opportunity to view and download child pornography. The Court will refer to Playpen, since the identity of the website has been widely publicized.

website. Special Agent Douglas Macfarlane, in his Affidavit in Support of Application for the NIT Search Warrant, stated:

Due to the unique nature of the Tor network and the method by which the network protects the anonymity of its users by routing communications through multiple computers or “nodes” . . . other investigative procedures that are usually employed in criminal investigations of this type have been tried and have failed or reasonably appear to be unlikely to succeed if they are tried.

[Dkt. No. 34-1, Affidavit in Support of Application for Search Warrant, at 28-29, ¶ 31].

On February 20, 2015, U.S. Magistrate Judge Theresa Carroll Buchanan issued the NIT warrant. When users accessed Playpen, the NIT caused data extraction software to be installed on the user’s computer – wherever it was located. The computer then sent – without Defendant’s knowledge or permission – requested information to a Government-controlled computer.<sup>4</sup> In this way, the Government could determine the identity of the person accessing Playpen – even when that person was using a computer that was located outside the Eastern District of Virginia.

Using NIT, agents determined that a Playpen registrant with the user name “johnnyb5” and an IP address of 70.177.122.133 had logged on to the website from February 20 to March 4, 2015. Agents were able to determine that the IP address was operated by Cox Communications, Inc. Using an administrative subpoena directed at Cox, they secured the name and address of the account holder. This information was included in the affidavit of Special

---

<sup>4</sup> This information included the IP address of the home computer, its type of operating system, the computer’s “Host Name”, its active operating system username and its media access control (“MAC”) address.

Agent Joseph Cecchini in support of a search warrant application presented to U.S. Magistrate Judge T. Lane Wilson in the Northern District of Oklahoma (the “Oklahoma warrant”) on November 2, 2015. *See* 15-mj-196-TLW, [Dkt. 1]. The affidavit supporting the Oklahoma warrant is quite similar to the affidavit supporting the NIT warrant application. However, the Oklahoma warrant details the Defendant’s alleged conduct regarding the Playpen website and the information obtained as a result of the NIT.

Judge Wilson issued the search warrant for 1515 S. Nyssa Place, Broken Arrow, Oklahoma. Agents executed the warrant, and located and seized alleged child pornography. Judge Wilson then executed a Criminal Complaint and a warrant for the Defendant’s arrest.

Defendant appeared before the undersigned on November 16, 2015, at which time, he was released on conditions of supervision.

Defendant’s Motion to Suppress seeks to preclude use of any material discovered through the search of his home, arguing, *inter alia*, that the warrant issued by the magistrate judge in Virginia is fatally flawed, and, thus, taints the Oklahoma warrant.

Plaintiff offers three arguments in support of his Motion to Suppress:

- First, that the magistrate judge in Virginia exceeded her authority under Fed. R. Crim. P. 41 by issuing a warrant for property outside her jurisdiction.

- Second, that the affidavit supporting the NIT warrant application falsely represented that the Playpen home page contained a depiction of “prepubescent females, partially clothed with their legs spread.”
- Third, the NIT warrant was overbroad because there was not probable cause to justify a search of all “activating computers” on the mere basis of registering with Playpen.

### **III. APPLICABLE LEGAL PRINCIPLES**

Clearly, a search occurs within the meaning of the Fourth Amendment when “the Government obtains information by physically intruding on a constitutionally protected area.” *U.S. v. Jones*, -- U.S. --, 132 S.Ct. 945, 950 n.3 (2012). However, the Fourth Amendment is not concerned just with “trespassory intrusions” on property. *Id.*, at 954 (Sotomayor, J. concurring). The reach of the Fourth Amendment does not “turn upon the presence or absence of a physical intrusion.” *Id.* (citing *Katz v. U.S.*, 389 U.S. 347, 353 (1967)). As Justice Sotomayor pointed out in *Jones*, we now have a variety of forms of electronic and other “novel modes” of surveillance that do not depend upon a physical intrusion of one’s property. Such is the case presented here, where it may not be entirely clear what “property” is being searched or seized or even where that search or seizure occurred.

The Fourth Amendment provides:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly

describing the place to be searched, and the person or things to be seized.

U.S. Const. amend. IV.

A search occurs “when the Government acquires information by either ‘physically intruding’ on persons, houses, papers or effects,’ ‘or otherwise invading an area in which the individual has a reasonable expectation of privacy.’” *U.S. v. Scully*, 108 F.Supp.3d 59, 75 (E.D.N.Y. 2015). “A seizure occurs when the Government interferes in some meaningful way with the individual’s possession of property.” *Id.* (quoting *U.S. v. Ganius*, 755 F.3d 125, 133 (2d Cir. 2014)). Pursuant to the Federal Rules of Criminal Procedure, the term “property” includes “documents, books, papers, any other tangible objects, and *information*.” Fed. R. Crim. P. 41(a)(2)(A) (emphasis added). The Rule permits seizure of electronic and digital data. “Rule 41 is sufficiently broad to include seizures of intangible items such as dial impulses...” *U.S. v. New York Tel. Co.*, 434 U.S. 159, 170 (1977).

The legality of a search is predicated upon a finding that the warrant authorizing the search comports with constitutional requirements and the provisions of Rule 41 which is “designed to protect the integrity of the federal courts or to govern the conduct of federal officers.” *U.S. v. Pennington*, 635 F.2d 1387, 1389 (10th Cir. 1980) (quoting *U.S. v. Millar*, 543 F.2d 1280, 1284 (10th Cir. 1976) and *U.S. v. Sellers*, 483 F.2d 37, 43 (5th Cir. 1973), *cert. denied*, 417 U.S. 908 (1974)).

Rule 41 provides in pertinent part:

**Authority to Issue a Warrant.** At the request of a federal law enforcement officer or an attorney for the government:

- (1) a magistrate judge with authority in the district ... has authority to issue a warrant to search for and seize a person or property located within the district;
- (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;
- (3) a magistrate judge -- in an investigation of domestic terrorism or international terrorism -- with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;
- (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and
- (5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:
  - (A) a United States territory, possession, or commonwealth;
  - (B) the premises – o matter who owns them – of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or
  - (C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

Fed. R. Crim. P. 41(b)(1)-(5).<sup>5</sup>

If the court finds a violation of Rule 41, this does not automatically mean the evidence seized must be suppressed. “Suppression of evidence ... has always been our last resort, not our first impulse.” *U.S. v. Leon*, 468 U.S. 897, 907 (1984). The exclusionary rule generates “substantial social costs,” which sometimes include setting the guilty free and the dangerous at large. We have therefore been “cautio[us] against expanding” it, and “have repeatedly emphasized that the rule’s ‘costly toll’ upon truth-seeking and law enforcement objectives presents a high obstacle for those urging [its] application,” *Pennsylvania Bd. of Probation and Parole v. Scott*, 524 U.S. 357, 364–365 (1998) (internal citations omitted).

#### **IV. RECENT CASES**

Several recent decisions arising from the same facts and circumstances before this Court are instructive. These include: *U.S. v. Michaud*, 2016 WL 337263 (W.D.Wash. Jan. 28, 2016); *U.S. v. Stamper*, Case No. 1:15cr109 (S.D.Ohio Feb. 19, 2016); *U.S. v. Epich*, 2016 WL 953269 (E.D.Wis. March 14, 2016); and, *U.S. v. Levin*, 2016 WL 1589824 (D.Mass. April 20, 106).

All of these cases involve the same “sting” operation that netted Defendant Arterbury. All of the cases involve the NIT warrant that was issued by a magistrate judge in the Eastern District of Virginia. In each case, the NIT warrant sent computer malware to an “activating computer” in a district

---

<sup>5</sup> Here, the warrant was issued pursuant to Rule 41(b)(1) – requesting a search/seizure of property “located in the Eastern District of Virginia.” [Dkt. No. 34-1, at 3].



outside of Virginia. That malware seized control of the defendants' computers and caused them to send identifying information to another Government computer in the Eastern District of Virginia. That identifying information was then used to secure a second warrant from a magistrate judge in the defendant's home district authorizing the search and seizure of the defendant's computer.

All of these four cases found that the NIT warrant violated Fed. R. Crim. P. 41(b). However, in *Michaud* and *Stamper*, the courts held that the violation of Rule 41 was a mere "technical violation" that did not prejudice the defendant. *Stamper* adopted the reasoning of *Michaud* that one has no reasonable expectation of privacy in one's IP address and such information, even when extraordinary means have been taken to secret that information. *Michaud* likened the IP address to an unlisted telephone number and opined that the Government would have ultimately been able to get this information without the NIT process.<sup>6</sup>

*Epich* is of little assistance to this Court because it is governed by Seventh Circuit law holding that "violations of federal rules do not justify the exclusion of evidence that has been seized on the basis of probable cause...." *U.S. v. Cazares-Olivas*, 515 F.3d 726, 730 (7th Cir. 2008). "The remedy of allowing a defendant to go free based on a violation of Rule 41's requirements for obtaining a proper search warrant would be 'wildly out of proportion to the

---

<sup>6</sup> I find this conclusion wholly at odds with the Affidavit submitted in support of the NIT warrant wherein the Government stated that absent use of the NIT, it would be impossible to secure the IP address.

wrong’.” *U.S. v. Berkos*, 543 F.3d 392, 396 (7th Cir. 2008) (quoting *Cazares-Olivas*, 515 F.3d at 730)).

In light of *Leon*, it is difficult to anticipate any violation of Rule 41, short of a defect that also offends the Warrant Clause of the Fourth Amendment, that would call for suppression. Many remedies may be appropriate for deliberate violations of the rules, but freedom for the offender is not among them.

*U.S. v. Trost*, 152 F.3d 715, 722 (7th Cir. 1998) (quoting *U.S. v. Hornick*, 815 F.2d 1156, 1158 (7th Cir. 1987)).

The Tenth Circuit does not follow the Seventh Circuit in this regard. In *Krueger*, for example, the Tenth Circuit suppressed evidence on the basis of a Rule 41(b) violation; thus, *Epich* is of little assistance to the Court’s analysis.

The remaining case is *Levin*, in which the district court – relying heavily on *Krueger* – found a fundamental jurisdictional defect in issuing the NIT warrant in violation of the provisions of Rule 41(b). Because the NIT warrant was void *ab initio*, the Court held, the good faith exception did not apply and the evidence had to be suppressed.

## **V DISCUSSION**

Because the undersigned believes that the validity of the NIT warrant issued in Virginia is determinative of the Defendant’s motion, the Court has focused its attention on that issue and the coincident suppression/good faith issues.

The Court begins by addressing two preliminary issues. First, the warrant under challenge is the NIT warrant issued in the Eastern District of Virginia. That warrant provided probable cause for the issuance of the second, Oklahoma warrant. The Government admitted at the April 25 hearing, that if the NIT warrant is fatally flawed, there would not be probable cause to support the Oklahoma warrant.

Second, the Court seeks to clarify what “property” was seized pursuant to the NIT warrant. The Government contends that in accessing the Playpen website Arterbury sent “packets of data” into the Eastern District of Virginia, and that this digital or electronic data is the property at issue. The Defendant contends that his home computer was the seized property. Essentially, he contends that the computer was first seized pursuant to the NIT warrant when the government, through malware, entered his home, took control of his computer and “searched” it for private information he had endeavored to keep confidential. Subsequently, the computer was physically seized when agents took it pursuant to the Oklahoma warrant.

The Court holds that the property seized was Arterbury’s computer. The Government did not seize the “packets of data” Arterbury sent to the Eastern District of Virginia, because it was unable to do so. Since there was no way to get this data, the Government employed the NIT to seize Arterbury’s computer and direct it to provide the identifying information without his knowledge. Had the Government seized Arterbury’s encrypted information in the Eastern District of Virginia, and, through some sort of forensic tool, un-encrypted it to

learn his identifying information, the Court would be inclined toward the Government's position, but that is not what happened. The Macfarlane affidavit makes it clear that the Government could not obtain Arterbury's IP address until its malware made its way back to his computer in Oklahoma and directed it to provide information to the Government.

**A. The Virginia Judge Lacked Rule 41 Authority to Issue the NIT Warrant.**

Defendant contends that the magistrate judge in Virginia lacked authority under Fed. R. Crim. P. 41 to issue a warrant seeking to seize/search property outside her judicial district. Rule 41 provides five grounds authorizing a magistrate judge to issue a warrant. Rule 41(b)(1)-(5). The parties agree that subsections (b)(3) and (b)(5) have no application here. Thus the analysis will be confined to subsections (b)(1), (b)(2) & (b)(4).

Subsection 41(b)(1) does not provide authority for the Virginia warrant because Arterbury's computer was not located in or seized in the Eastern District of Virginia.

The Government argues that subsections (b)(2) & b(4) provide authority for the NIT warrant. The Court disagrees.

Subsection (b)(2) applies where a judge signs a warrant to seize property that is within his/her jurisdiction at the time the warrant is signed, but has been re-located outside that jurisdiction at the time the warrant is actually executed. The Government contends that by electronically reaching into the Eastern District of Virginia, Arterbury brought "property" into that district that was subject to the NIT warrant. The Government argues that the property was

then removed from Virginia to Oklahoma, thus, the NIT warrant comports with subsection (b)(2).

The Court is not persuaded by this argument. The property seized in this instance was Arterbury's computer, which at all relevant times remained in Oklahoma. The NIT warrant allowed the Government to send computer code or data extraction instructions to Arterbury's computer, wherever it was located. The Government "seized" that computer and directed it to send certain information to the Government – all without Arterbury's knowledge or permission. Arterbury's computer was never in the Eastern District of Virginia and subsection (b)(2), therefore, does not apply. Furthermore, even if the property seized was electronic information, that property was not located in the Eastern District of Virginia at the time the warrant was signed. This information only appeared in Virginia *after* the Warrant was signed and executed and the Government seized control of Defendant's computer in Oklahoma.

The Court is also unpersuaded by the Government's argument that the NIT warrant is valid under Rule 41(b)(4) as a "tracking warrant." The NIT did not track Defendant's computer as it moved. In *Michaud*, the district court rejected the Government's argument as applied to the same NIT operation, stating, "If the 'installation' occurred on the government-controlled computer, located in the Eastern District of Virginia, applying the tracking device exception breaks down, because Mr. Michaud never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular

district,” and “[i]f the installation occurred on Mr. Michaud’s computer, applying the tracking device exception again fails, because Mr. Michaud’s computer was never physically located within the Eastern District of Virginia.” This Court agrees with *Michaud* in this regard and concludes Subsection 41(b)(4) is not applicable. The NIT warrant was not for the purpose of installing a device that would permit authorities to track the movements of Defendant or his property.

Furthermore, the drafters of Rule 41 knew how to avoid the territorial limit on issuance of warrants when they wished to do so. Rule 41(b)(3) removes the territorial limitation in cases involving domestic or international terrorism. In such cases, a magistrate judge “with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district.” Rule 41(b)(3). The drafters of Rule 41 could easily have included child pornography in Rule 41(b)(3) and, thereby, avoided the territorial limitation of Rule 41(b)(1) & (2). They did not do so. The Court can only conclude that they did not intend to remove the territorial limit in cases such as the one before the Court.

Authority to issue warrants exists only insofar as granted by the rules, and no further. Accordingly, just as the court concluded in *Michaud*, this Court finds that the NIT warrant was not authorized by any of the applicable provisions of Rule 41.<sup>7</sup> Thus, the court concludes that the issuance of the

---

<sup>7</sup> Apparently, the Government is aware of the problem of authorizing NIT warrants under the current Rules of Criminal Procedure. The Department of Justice has proposed amendments to Rule 41 that would resolve this issue.

warrant violated Rule 41(b).<sup>8</sup>

**B. The Virginia Judge Lacked Authority Under the Federal Magistrate Judges Act.**

There is another fundamental problem with the Virginia magistrate judge's authority to issue the NIT warrant. As Judge Gorsuch noted in his concurring opinion in *Krueger*, the Government's problem goes to the heart of the magistrate judge's statutory source of power. The Federal Magistrate Judges Act provides three territorial limits on a magistrate judge's power:

Each United States magistrate judge serving under this chapter shall have [1] within the district in which sessions are held by the court that appointed the magistrate judge, [2] at other places where that court may function, and [3] elsewhere as authorized by law ... all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts....

*Id.* at 1118 (citing 28 U.S.C. § 636(a)).<sup>9</sup>

As in *Krueger*, the magistrate judge “purported to exercise power in none of these places.” 809 F.3d at 1118. Thus, Judge Gorsuch notes, “The warrant on which the government seeks to justify its search in this case was no warrant at all when looking to the statutes of the United States.” *Id.* (emphasis added).

<sup>8</sup> Defendant also asserts the NIT Warrant lacked statutory jurisdiction and therefore violated the Fourth Amendment. [Dkt. No. 33 at pp. 10-11 (citing Judge Gorsuch's concurring opinion in *Krueger*, 809 F.3d at 1117-26)]. However, consistent with the majority opinion in *Krueger*, since the court has determined that there was a clear Rule 41(b) violation, it declines to reach this issue. *Id.* at 1104-05 (“[C]onsistent with the fundamental rule of judicial restraint, we decline to reach a constitutional question that is not necessary for our resolution of this appeal (citation omitted)).

<sup>9</sup> In *Krueger*, the government secured a warrant from a magistrate judge in Kansas permitting the seizure and search of property located in Oklahoma. The Tenth Circuit affirmed the lower court's finding that the warrant violated Rule 41 and the court's suppression of the evidence seized pursuant to the invalid warrant. See, discussion at p. 19-21, *infra*.

**C. Under *Krueger*, Suppression is Warranted Because the Search Would Not Have Occurred But For the Breach of Rule 41(b).**

The court must next consider whether suppression is justified. To establish the case for suppression, Defendant must show that he was prejudiced by the violation of Rule 41. The prejudice standard adopted in *Krueger* allows defendant to show either “(1) prejudice in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) intentional disregard for a provision of the Rule.” *Krueger*, 809 F.3d at 1115 (citing *United States v. Pennington*, 635 F.2d 1387, 1390 (10th Cir. 1980)). As set forth above, the court does not address whether the warrant fails for constitutional reasons, but limits its analysis to the violation of Rule 41(b). Specifically, does a violation of Rule 41(b) justify suppression of evidence?

In *Krueger*, the Tenth Circuit addressed this question for the first time. (“The Court has not yet had occasion to consider whether suppression is justified when a warrant is issued by a federal magistrate judge who clearly lacks authority to do so under Rule 41(b)(1).” *Krueger*, 809 F.3d at 1115). The court answered that question affirmatively.

In *Krueger*, a Homeland Security Investigations (“HSI”) agent learned that child pornography was being distributed over the internet from an IP address registered to Krueger, a Kansas resident. *Id.* at 1111. The agent obtained a warrant (“Warrant 1”) from a United States magistrate judge in the District of Kansas to search defendant Krueger’s Kansas residence for items such as



computers and cell phones that might be used to depict child pornography. *Id.* Upon executing the warrant, the agent was told by Krueger's roommate that Krueger was in Oklahoma City and may have taken his computer and cell phone with him. *Id.* After an HSI agent in Oklahoma verified Krueger's whereabouts, the agent in Kansas sought and obtained a second warrant ("Warrant 2") from a different magistrate judge in the District of Kansas. *Id.* The second warrant authorized law enforcement to search the Oklahoma residence where Krueger was staying and Krueger's automobile. The warrant was immediately transmitted to an HSI agent in Oklahoma, who executed the warrant and seized Krueger's computer and external hard drive. *Id.* A subsequent search of the devices revealed evidence that Krueger had downloaded and traded child pornography using his peer-to-peer networking account and, as a result, Krueger was charged with distribution of child pornography in violation of 18 U.S.C. § 2252(a)(2). *Id.* at 1112. Krueger filed a motion to suppress, asserting Warrant 2 violated Rule 41(b)(1) because the magistrate judge in the District of Kansas did not have authority to issue a warrant for property already located in Oklahoma. *Id.* After a suppression hearing, the district court granted the motion, concluding that the warrant violated Rule 41(b)(1) and Krueger had demonstrated prejudice in the sense that the Kansas magistrate judge would not have issued Warrant 2 had Rule 41 "been followed to the letter." *Id.* at 1112-13.

On appeal, the Government conceded that Warrant 2 violated Rule 41(b)(1) because the magistrate judge in Kansas had no authority to issue a

warrant for property already located in Oklahoma but argued the district court applied the wrong legal standard in determining that Krueger demonstrated prejudice as a result of the violation. *Id.* at 1113. The Government asserted the appropriate question was not whether any judge in the District of *Kansas* could have issued Warrant 2, but instead was whether any judge in the Western District of *Oklahoma* could had issued the warrant. *Id.* at 1116. The Tenth Circuit disagreed, concluding the Government’s proposed approach was too speculative. *Id.* It stated, “[I]nstead of focusing on what the Government *could have* done to comply with Rule 41(b)(1), we conclude that prejudice in this context should be anchored to the facts as they actually occurred.” *Id.* Accordingly, it adopted the district court’s standard for determining whether defendant had established prejudice and asked “whether the issuing federal magistrate judge could have complied with the Rule.” *Id.*

The Government argues *Krueger* is inapposite because there, the agent knew the exact location of the evidence being sought, and was aware the location was in Oklahoma, when he obtained Warrant 2 from a Kansas magistrate judge. Here, in contrast, the agent did not know and could not have known the physical location of Playpen registrants due to the affirmative steps taken by Playpen administrators and users to conceal their illegal activity.

The Government’s position finds some support in *Michaud, supra*. In *Michaud*, the district court concluded that although a technical violation of Rule 41 had occurred, suppression was not warranted because the record did

not show that defendant was prejudiced or that the FBI acted intentionally and with deliberate disregard of Rule 41(b). Applying the Ninth Circuit’s definition of prejudice, i.e., “prejudice ‘in the sense that the **search** would not have occurred . . . if the rule had been followed,’” the district court found that the defendant had “no reasonable expectation of privacy of the most significant information gathered by deployment of the **NIT**, Mr. Michaud’s assigned IP address, which ultimately led to Mr. Michaud’s geographic location.” *Id.* at \*\*6-7. Furthermore, the court concluded that “[t]he IP address was public information, like an unlisted telephone number, and eventually could have been discovered.” *Id.* at \*7.<sup>10</sup>

The Tenth Circuit’s definition of “prejudice” – i.e., “prejudice in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed” – is similar to the Ninth Circuit definition. *See Krueger*, 809 F.3d at 1115. Here, the searches of Arterbury’s computer would not have occurred had Rule 41(b) been followed. Absent deployment of the NIT, the physical location of Playpen registrants was not discoverable. *See Macfarlane Affidavit*, Dkt. No. 34-1]. Under the *Krueger/Pennington* framework, the evidence must be suppressed. Rule 41 was clearly violated, and the Oklahoma search would not have occurred had Rule 41(b) been

---

<sup>10</sup> The court in *Michaud* offered no citation or support for these conclusions. The court indicated that the Government would have no difficulty discovering the IP address for an individual using the Tor network. This is contrary to the undersigned’s understanding of how the Tor network works and is specifically contradicted by the statements set forth in Special Agent Macfarlane’s Affidavit seeking the NIT Warrant in the Eastern District of Virginia. [Dkt. No. 34-1, ¶¶ 8, 9, & 31].

followed. Furthermore, *Krueger* articulates the appropriate inquiry as whether any magistrate judge in the Eastern District of Virginia could have complied with Rule 41 given the facts of this case. The answer to that question is “no.”

The Government also argues that there was no prejudice to Arterbury because he had no reasonable expectation of privacy in his IP address. The Government asserts that the IP address is actually the property of the Internet Service Provider, and that one must disclose this IP address to a third-party in order to access the Internet. Were the IP address obtained from a third-party, the Court might have sympathy for this position. However, here the IP address was obtained through use of computer malware that entered Defendant’s home, seized his computer and directed it to provide information that the Macfarlane affidavit states was unobtainable in any other way. Defendant endeavored to maintain the confidentiality of his IP address, and had an expectation that the Government would not surreptitiously enter his home and secure the information from his computer.

**D. The “Good Faith Exception Does Not Apply.”**

The most troubling aspect of this case is whether suppression of evidence can be avoided through application of the “good-faith” exception to the exclusionary rule. Having determined that the NIT warrant was void as against Arterbury, the Court must determine whether suppression of the evidence found during the search of his home is warranted. In *U.S. v. Leon*, 468 U.S. 897 (1984), and its companion case, *Mass. v. Sheppard*, 468 U.S. 981 (1984), the Supreme Court recognized a “good faith” or *Leon* exception to the Fourth

Amendment exclusionary rule.<sup>11</sup> Under the *Leon* exception, evidence obtained pursuant to a warrant later found to be invalid may be introduced in the government's case-in-chief at the defendant's trial, if a reasonably well-trained officer would have believed that the warrant was valid. The premise for the exception is that there is inadequate justification to apply the exclusionary rule when police obtain a warrant, reasonably relying on its validity, only to later learn that the judge erred in authorizing the search. The court noted in *Leon*, "Penalizing the officer for the magistrate's error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations." *Leon*, 468 U.S. at 921.

In *Krueger*, the Tenth Circuit held that violation of Rule 41(b) justified suppression of evidence; however, *Krueger* dealt with a single warrant – a warrant issued by a Kansas magistrate judge authorizing search and seizure of property in Oklahoma. This case – and those cited above in ¶IV – presents a different scenario: a second warrant is secured in the appropriate jurisdiction, but probable cause for the second warrant was secured by means of an earlier, invalid warrant. Should the good-faith exception permit officers to rely on the second, valid warrant? Or is the second warrant fatally flawed because of the invalidity of the first warrant?

---

<sup>11</sup> *Leon* "contemplated two circumstances: one in which a warrant is issued and is subsequently found to be unsupported by probable cause and the other in which a warrant is supported by probable cause, but is technically deficient." *U.S. v. Levin*, 2016 WL 1589824 (D.Mass. April 20, 2016) (quoting *U.S. v. Vinnie*, 683 F.Supp. 285, 288 (D. Mass. 1988)).

The Government first contends that the *Leon* exception should apply here because the NIT warrant is a “technical violation” of Rule 41(b). The Court rejects the notion that this case presents nothing more than a “technical violation” of Rule 41. It is true that courts have found that suppression is not warranted in some cases of a Rule 41 violation; however, these have generally involved violations of procedural requirements under Rule 41(a), (c), (d), or (e). *E.g.*, *U.S. v. Rome*, 809 F.2d 665 (10th Cir. 1987) (violation of Rule 41(c)). *See Krueger*, 809 F.3d at 1115, n.7 (collecting cases). However, in this case the violation of Rule 41 goes to the fundamental jurisdiction and “substantive judicial authority” of the magistrate judge to issue the NIT warrant. *Krueger*, 809 F.3d at 1115, n.7 (*citing Berkos*, 543 F.3d at 397).

In *Levin*, the Court relied on *Krueger* and *Berkos* to distinguish technical violations of Rule 41 from the type of violation presented here:

Rule 41, however, has both procedural and substantive provisions — and the difference matters. Courts faced with violations of Rule 41's procedural requirements have generally found such violations to be merely ministerial or technical, and as a result have determined suppression to be unwarranted. By contrast, this case involves a violation of Rule 41(b), which is “a substantive provision[.]” *United States v. Berkos*, 543 F.3d 392, 398 (7th Cir. 2008); *see also United States v. Krueger*, 809 F.3d 1109, 1115 n.7 (10th Cir. 2015) (noting that Rule 41(b)(1) “is unique from other provisions of Rule 41 because it implicates substantive judicial authority,” and accordingly concluding that past cases involving violations of other subsections of Rule 41 “offer limited guidance”) (internal quotation marks and citation omitted). Thus, it does not follow from cases involving violations of Rule 41's procedural provisions that the Rule 41(b) violation at issue here — which involves the authority of the magistrate judge to issue the warrant, and consequently, the underlying validity of the warrant — was simply ministerial. *See United States v. Glover*, 736 F.3d 509, 515 (D.C. Cir. 2013) (concluding that a Rule 41(b) violation constitutes

a “jurisdictional flaw” that cannot “be excused as a ‘technical defect’”).

*Levin*, 2016 WL 1589824, at \*7

In *Krueger*, the trial Court noted, “[I]t is quite a stretch to label the government's actions in seeking a warrant so clearly in violation of Rule 41 as motivated by ‘good faith.’ ” *U.S. v. Krueger*, 998 F.Supp.2d 1032, 1036 (D.Kan. 2014) (quoting *U.S. v. Glover*, 736 F.3d 509, 516 (D.C.Cir. 2013)).

*Levin* concluded that the good-faith exception was inapplicable to a warrant held to be void *ab initio* under Rule 41(b). *Id.* Other courts have indicated, in dicta, that where evidence is obtained pursuant to a warrant that is void *ab initio*, the good-faith exception does not apply. *See, Levin*, at \*10 & n.17 (collecting cases). *See also, State v. Wilson*, 618 N.W.2d 513, 520 (S.D. 2000) (good-faith exception inapplicable to warrant by state judge acting outside territorial jurisdiction); *State v. Nunez*, 634 A.2d 1167, 1171 (D.R.I. 1993) (good faith exception would not apply to a warrant that is void *ab initio*).

Based on the holdings of *Krueger* and *Levin*, I conclude that where the Rule 41 violation goes directly to the magistrate judge’s fundamental authority to issue the warrant, as in the violation presented here, it is not a “technical violation” of the Rule. The warrant is void *ab initio*, suppression is warranted and the good-faith exception is inapplicable.

The Government also argues that because of exigent circumstances the NIT search would have been justified, even had the magistrate judge in Virginia refused to sign it. The Court is not persuaded by this argument either. The

exigent circumstances were the on-going downloading and distribution of child pornography. In this instance, the specific activity at issue was on-going only because the Government opted to keep the Playpen site operating while it employed the NIT. The Government cannot assert exigent circumstances when it had a hand in creating the emergency.

Exclusion of the evidence in this case will serve the remedial and prophylactic purposes of the exclusionary rule, by serving notice to the Government that use of an NIT warrant under the circumstances presented here exceeds a magistrate judge's authority under the Federal Magistrate Judges Act and Rule 41(b) of the Rules of Criminal Procedure.

The NIT Warrant clearly did not comport with Fed. R. Crim. P. 41(b), and, therefore, was invalid *ab initio*. Arterbury was prejudiced by issuance of the NIT Warrant and the Court finds no basis for application of the good faith exception to the exclusionary rule. Accordingly, Defendant's motion to suppress [Dkt. No. 33] must be granted.<sup>12</sup>

## **V. CONCLUSION**

The purpose of Rule 41 is to carry out the mandate of the Fourth Amendment. It binds federal courts and federal law enforcement officers. *Navarro v. U.S.*, 400 F.2d 315, 318-19 (5th Cir 1968), *overruled on other grounds*, *U.S. v. McKeever*, 905 F.2d 829, 833 (5th Cir. 1990)):

---

<sup>12</sup> Having determined the United States magistrate judge in Virginia exceeded her authority under Fed. R. Crim. P. 41, the court declines to address defendant's remaining arguments in support of suppression.



The obligation of the federal agent is to obey the Rules. They are drawn for the innocent and guilty alike. They prescribe standards for law enforcement. They are designed to protect the privacy of the citizen, unless the strict standards set for searches and seizures are satisfied. That policy is defeated if the federal agent can flout them and use the fruits of his unlawful act either in federal or state proceedings.

*Rea v. United States*, 350 U.S. 214, 217-18 (1956).

- The NIT warrant was issued in violation of Rule 41(b).
- The violation was not a “technical violation” because it implicates “substantive judicial authority.” *Krueger*, 809 F.3d at 1115, n.7.
- The NIT warrant was, therefore, void *ab initio*. *Levin*, at \*8.
- The *Leon* exception does not apply when an underlying warrant is void *ab initio*. *Levin*, at \*11-\*12.

Accordingly, for the reasons set forth above, I recommend the Defendant’s Motion to Suppress [Dkt. No. 33] be **GRANTED**.

### **OBJECTIONS**

The District Judge assigned to this case will conduct a de novo review of the record and determine whether to adopt or revise this Report and Recommendation or whether to recommit the matter to the undersigned. As part of his/her review of the record, the District Judge will consider the parties’ written objections to this Report and Recommendation. In order to expedite this matter for consideration by the District Judge, the period for objections must be shortened. *See* Fed. R. Crim P. 59(b). Therefore, a party wishing to file objections to this Report and Recommendation must do so **by May 2, 2016**. *See* 28 U.S.C. § 636(b)(1) and Fed. R. Crim. P. 59(b). The failure to file timely

written objections to this Report and Recommendation waives a party's right to review. Fed. R. Crim P. 59(b).

**DATED** this 25<sup>th</sup> day of April 2016.

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

<b>UNITED STATES OF AMERICA,</b>	)	
	)	
<b>Plaintiff,</b>	)	
	)	
<b>v.</b>	)	<b>Case No. 15-CR-182-JHP</b>
	)	
<b>SCOTT FREDRICK ARTERBURY</b>	)	
	)	
<b>Defendant.</b>	)	

**ORDER AFFIRMING AND ADOPTING THE REPORT  
AND RECOMMENDATION OF THE UNITED STATES  
MAGISTRATE JUDGE**

On April 25, 2016 the United States Magistrate Judge entered a Report and Recommendation (Doc. No. 42) regarding Defendant’s Motion to Suppress Evidence Seized from Residence (Doc. No. 33). The Magistrate Judge recommended that Defendant’s Motion to Suppress be granted.

On May 2, 2016, the United States timely filed its objections to the Magistrate Judge’s Report and Recommendation (Doc. No. 44), to which the Defendant responded (Doc. No. 45).

Upon full consideration of the entire record and the issues presented therein, this Court finds and orders that the Report and Recommendation entered by the United States Magistrate Judge on April 25, 2016, is supported by the record and is **AFFIRMED** and **ADOPTED** by this Court as its Findings and Order. Therefore the Defendant’s Motion to Suppress Evidence Seized from Residence is **GRANTED**.

The case remains set for jury trial on Tuesday, May 17, 2016 at 9:30 am.

**IN THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF OKLAHOMA**

<b>UNITED STATES OF AMERICA,</b>	)	
	)	
<b>Plaintiff,</b>	)	
	)	
<b>v.</b>	)	<b>Case No. 15-CR-000182-JHP</b>
	)	
<b>SCOTT FREDRICK ARTERBURY,</b>	)	
	)	
<b>Defendant.</b>	)	

**UNITED STATES’ MOTION FOR RECONSIDERATION OF THE  
COURT’S ORDER SUPPRESSING EVIDENCE**

The United States of America, by and through counsel, Danny C. Williams, Sr., United States Attorney for the Northern District of Oklahoma, and Andrew J. Hofland, Assistant United States Attorney, respectfully moves this Court to reconsider its May 12, 2016 Order (Doc. 47) that adopted the Magistrate Judge’s Report and Recommendation (Doc. 42) and granted Defendant Scott Fredrick Arterbury’s Motion to Suppress Evidence (Doc. 25). *United States v. Hardy*, No. 07-MJ-108-FHM, 2008 WL 5070945, at \*1 (N.D. Okla. Nov. 21, 2008) (“A district court has inherent authority to reconsider its rulings as long as it retains jurisdiction over a matter.” (internal quotation omitted)). The Order granting suppression merits reconsideration for the following reasons:

ARGUMENT AND AUTHORITY

**1. The NIT warrant was not void *ab initio*.**

The court’s threshold determination that the NIT Warrant was void from the outset because the magistrate judge was without authority to issue it is incorrect. First, even assuming, without conceding, that Rule 41 did not permit the magistrate judge to issue a warrant for the search of activating computers located in other federal districts, the warrant was not wholly void because Rule 41 plainly authorized

the magistrate judge to issue the NIT Warrant for the search of activating computers located within the Eastern District of Virginia and within a territory, possession, or commonwealth of the United States and diplomatic or consular premises and residences of the United States located in foreign states. *See* Fed. R. Crim. P. 41(b)(1) and (5). Second, the Rule 41 violation that the Court found to have occurred in this case—essentially, that the government obtained authorization for the NIT Warrant from the wrong judge in the right district—does not implicate the Fourth Amendment and therefore does not render the warrant utterly void without regard to whether the defendant suffered prejudice. For both of these reasons, the Court’s finding that the NIT Warrant was void *ab initio* must be reconsidered.

As argued in its opposition to the defendant’s motion to suppress, the United States maintains that the magistrate judge was authorized pursuant to Rule 41(b) (and ultimately, 28 U.S.C. § 636(a)) to issue the NIT warrant to search for activating computers, wherever located, that accessed Playpen to view, download, and distribute child pornography. However, even accepting for the purposes of this motion the court’s finding that § 636(a) and Rule 41(b) did not permit the magistrate judge to issue a warrant for the search of activating computers that were located in other districts, the court’s finding that the magistrate judge was wholly without authority to approve the NIT warrant is erroneous. In fact, Rule 41(b) permitted the magistrate judge, at a minimum, to issue the NIT warrant for the search of activating computers located within the Eastern District of Virginia and within the territorial and diplomatic areas listed in subsection (5). Since the magistrate judge acted well within her authority to approve the search warrant for these locations, it cannot be said that “there simply was no judicial approval” for the warrant. *See* Doc. 42 at 18.

As a threshold matter, the NIT warrant satisfied the Fourth Amendment's warrant requirements in all respects. As laid out in the United States' Response (Doc. 34), the NIT warrant application established probable cause to search the activating computers of users who intentionally logged on to the Target Website to view, download, and disseminate child pornography. Further, the warrant application particularly described the things to be seized. And the defendant does not claim that the magistrate judge to whom the warrant was presented was not "neutral and detached," as required to ensure the protections afforded by the Fourth Amendment, *Johnson v. United States*, 333 U.S. 10, 14 (1948), or was not duly appointed and authorized to perform all of the functions of a United States magistrate judge in the Eastern District of Virginia. *See* 28 U.S.C. § 636.

Under these circumstances, the magistrate judge was clearly authorized, at a minimum, pursuant to § 636(a)(1) and Rule 41(b)(1) and (5) to issue the NIT warrant, which satisfied the Fourth Amendment's probable cause and particularity requirements, for the search of activating computers in the Eastern District of Virginia and United States' territories and diplomatic locations. Since the magistrate judge was permitted by statute and rule to issue the constitutional NIT warrant for searches within her jurisdiction, the court's finding that she had no authority to issue the warrant is unsound. That the NIT warrant could have been—and in fact was, *see, e.g., United States v. Darby*, No. 16-CR-36-RGD-DEM (E.D. Va. Jun. 3, 2016) (defendant charged with possession of child pornography after deployment of NIT to computer located in the Eastern District of Virginia identified him as a user of Website A)—validly executed in the Eastern District of Virginia distinguishes this case from *United States v. Krueger*, 809 F.3d 1109 (10th Cir. 2015), and *United States*

*v. Glover*, 736 F.3d 509 (D.C. Cir. 2013), which the Court relied upon to find the NIT warrant void *ab initio*.

In both *Krueger* and *Glover*, the warrant applications presented to the judge for approval made clear that the place to be searched was not within the authorizing judge's district. *Krueger*, 809 F.3d at 1111 (warrant presented to magistrate judge in the District of Kansas asked for permission to search home and vehicle located in Oklahoma); *Glover*, 736 F.3d at 510 (warrant presented to district court judge in the District of Columbia asked for permission to install tracking device on vehicle located in Maryland). As a consequence, the courts concluded that the warrants were invalid at the time they were issued because the territorial limitations of Rule 41 (and in *Glover*, of Title III) did not authorize the judges to issue warrants for searches in other districts. *Krueger*, 809 F.3d at 1116-17, 1118 (Gorsuch, J., concurring); *Glover*, 736 F.3d at 515. Here, in contrast, the NIT warrant application presented to the magistrate judge asked for permission to search the activating computers—"wherever located"—that accessed the Playpen server located in the Eastern District of Virginia. Unlike the warrants in *Krueger* and *Glover*, the NIT warrant did not specify that the search would occur only outside of the Eastern District of Virginia, and since the warrant also contemplated a search within the authorizing judge's district, it was presumptively valid at the time it was issued. *Cf. United States v. Moreno-Magana*, No. 15-CR-40058-DDC, 2016 WL 409227, at \*14-15 (D. Kan. Feb. 3, 2016) (distinguishing *Krueger* and rejecting claim that warrant issued by Kansas state court judge to search phone was void *ab initio* because, at time warrant was issued, precise location of phone was unknown; thus, unlike in *Krueger*, where both law enforcement and issuing magistrate knew that the property to be searched was not within the magistrate's district at time warrant was issued, "[t]he

warrants here did not authorize pinging of phones that the issuing judge knew to be outside Kansas”). The court should therefore reconsider its finding that the magistrate judge was without any legal authority to issue the NIT warrant.

**2. The defendant was not prejudiced by any Rule 41 violation and therefore is not entitled to suppression.**

Despite finding, on one hand, that the warrant was void *ab initio*, the court completes the Rule 41 suppression analysis in accordance with *United States v. Pennington*, 635 F.2d 1387, 1390 (10th Cir. 1980). The United States agrees that the proper factors to be first considered in determining whether suppression might be warranted for a Rule 41 violation are listed in *Pennington*. In that vein, and without proof of intentional or deliberate disregard for a provision of the Rule, the defendant must demonstrate that he suffered prejudice to merit suppression. *See, e.g., United States v. Michaud*, No. 15-CR-05351-RJB, 2016 WL 337263, at \*5-7 (W.D. Wash. Jan. 28, 2016) (rejecting claim that very same NIT warrant issued in this case required suppression due to Rule 41 violation and finding that violation was merely technical and defendant could not establish prejudice); *United States v. Stamper*, No. 15-CR-109-MRB, Doc. 48 at 21-23 (S.D. Ohio Feb. 19, 2016) (same); *United States v. Epich*, No. 15-CR-163-PP, 2016 WL 953269, at \*2 (E.D. Wis. Mar. 14, 2016) (discussing same NIT warrant issued in this case and noting that, even if violation of Rule 41 occurred, it did not require suppression); *United States v. Werdene*, No. 15-CR-434-GJP, Doc. 33 at 21 (E.D. Pa. May 19, 2016) (denying motion to suppress the same NIT warrant issued in this case because, in part, the defendant did not prove prejudice, defined in the Third Circuit as “offend[ing] concepts of fundamental fairness or due process”); *Darby*, 16-CR-36-RGD-DEM, Doc. 31 at 25 (E.D. Va. Jun. 3, 2016) (no prejudice when executed within the Eastern District of Virginia insofar as Rule 41(b)(1) would have authorized a search of the magistrate’s own district);



*United States v. Hernandez*, No. 08-198(1) (JRT/RLE), 2008 WL 4748576, at \*15-16 (D. Minn. Oct. 28, 2008) (finding issuance of constitutionally valid warrant by Minnesota state court judge for search of bank located in South Dakota to be technical violation that did not require suppression because defendant was not prejudiced); *United States v. Vann*, No. 07-CR-247 (JMR/RLE), 2007 WL 4321969, at \*22-23 (D. Minn. Dec. 6, 2007) (similar, where warrant issued by federal magistrate judge in the District of Minnesota for search of property in the Western District of Wisconsin); *United States v. LaFountain*, 252 F. Supp. 2d 883, 891 (D.N.D. 2003) (similar, where warrants issued by tribal court judge). As these cases make clear, violations of Rule 41(b), just like violations of Rule 41's other prerequisites, do not automatically require suppression without a showing of prejudice to the defendant. *See United States v. Burgos-Montes*, 786 F.3d 92, 108-09 (1st Cir. 2015), *cert. denied*, 136 S. Ct. 599 (2015) (finding that Rule 41(f)(1)(C) violation does not require suppression absent a showing of prejudice and noting that “[o]ther circuits have held the same applies to all the prerequisites of Rule 41”) (citing *United States v. Schoenheit*, 856 F.2d 74, 76-77 (8th Cir. 1988), and *United States v. Burke*, 517 F.2d 377, 386-87 (2d Cir. 1975)).

This Court interprets the *Krueger* definition of prejudice to say that the operative question is not what was possible but what factually happened in this instance. But this formulation of prejudice, however, “makes no sense, because under that interpretation, all searches executed on the basis of warrants in violation of Rule 41(b) would result in prejudice, no matter how small or technical the error might be. Such an interpretation would defeat the need to analyze prejudice separately from the Rule 41(b) violation.” *Michaud*, 2016 WL 337263, at \*6. As discussed above, there is no basis to treat Rule 41(b) violations differently from other Rule 41 violations and

the thus the Court’s prejudice formulation, which effectively eliminates the prejudice inquiry altogether by creating a per se rule of suppression for all Rule 41(b) violations, cannot stand.

Here, the defendant’s prejudice argument boils down to an assertion that, because he intentionally employed anonymizing technology to perpetrate his crimes against children in the shadows of the dark web, Rule 41(b) prohibits law enforcement from obtaining a warrant authorizing its use of the NIT to identify and locate him. That is not the sort of claimed “prejudice” that should result in suppression. The NIT warrant satisfied the Fourth Amendment’s probable cause and particularity requirements, and thus, had it been presented to a judge with authority to issue the warrant—such as a magistrate within the Northern District of Oklahoma—Rule 41 clearly would have authorized the very same search of the defendant’s computer that occurred. *See, e.g., Vann*, 2007 WL 4321969, at \*23 (“[T]he presence of probable cause for the issuance of the Warrant adequately demonstrates that the same Warrant would have been issued by a Magistrate Judge in the Western District of Wisconsin, if it had been presented for that Judge’s review.”); *Hernandez*, 2008 WL 4748576, at \*16 (same, involving issuance of warrant by state court judge without jurisdiction); *LaFountain*, 252 F. Supp. 2d at 891 (same, involving issuance of warrant by tribal court judge without jurisdiction).

Moreover, although it would have been difficult for the United States to identify the defendant’s IP address—the most significant information gathered by deployment of the NIT—without the NIT warrant, the IP address was public information in which the defendant had no reasonable expectation of privacy and thus it was obtainable by other lawful means. *Michaud*, 2016 WL 337263, at \*7. *Cf. United States v. Welch*, 811 F.3d 275, 281 (8th Cir. 2016) (finding no prejudice to defendant

from violation of Rule 41's notice provision because, had Rule 41 been followed, same search would have occurred and same evidence recovered). In short, had the court applied the proper standard for evaluating prejudice resulting from the Rule 41(b) violation, the record makes manifest that the defendant did not suffer prejudice and that suppression was not an appropriate remedy.

**3. The good-faith exception precludes suppression of evidence in this case.**

Even assuming, without conceding, that the warrant was void at the outset, suppression is not warranted. The court committed two errors in analyzing whether the evidence obtained pursuant to the NIT warrant should be suppressed, notwithstanding the United States' apparent good-faith reliance on the now-invalidated warrant. First, the Court erroneously concluded that the good-faith exception was inapplicable here because the deployment of the NIT was effectively a warrantless search. Second, the Court erroneously concluded that it was not objectively reasonable for law enforcement to have relied on the NIT warrant in executing the search. The record and relevant case law do not support either of those conclusions, and since suppression will serve only to punish law enforcement for a reasonable, if now deemed mistaken, interpretation of Rule 41(b) and will not serve to deter any future violation, the Court should reconsider its conclusion that suppression—a remedy of last resort—is required in this case.

First, as noted above, the warrant was not void *ab initio* because the magistrate judge had authority under both the Federal Magistrates Act and Rule 41(b) to issue the challenged warrant deploying the NIT, at a minimum, within the territorial limits of the Eastern District of Virginia and any possession, territory, or commonwealth of the United States and diplomatic or consular premises and residences of the United States located in foreign states. *See* Fed. R. Crim. P. 41(b)(1) and (5). Even

accepting the Court's finding that the NIT warrant violated Rule 41(b) by permitting a search beyond those geographic boundaries, the error was not one of constitutional magnitude, as it did not vitiate probable cause for the search or render the warrant insufficiently particular. Thus, although the warrant may be "voidable" due to the Rule 41 violation, it does not follow that it is wholly "void" and therefore suppression is automatic. Indeed, other courts have refused to suppress evidence obtained from the same NIT warrant issued in this case, finding that suppression was an inappropriate remedy where the Rule 41(b) violation did not undermine the constitutionality of the warrant and the government's reliance on the warrant was objectively reasonable. *See Michaud*, 2016 WL 337263, at \*7; *Stamper*, D.48 at 19-23; *Epich*, 2016 WL 953269, at \*2. Other courts have likewise refused to suppress evidence obtained from warrants that were later found invalid due to the issuing judge's lack of authority. *See, e.g., United States v. Master*, 614 F.3d 236, 242-43 (6th Cir. 2010); *Hernandez*, 2008 WL 4748576, at \*16-17; *Vann*, 2007 WL 4321969, at \*23; *LaFountain*, 252 F. Supp. 2d at 891-92. The analysis in those cases, although not binding on this Court, provides compelling reasons for this Court to reconsider its conclusion that the good-faith exception is inapplicable to this case.

Second, the Court's suppression order is inconsistent with the Supreme Court's recent exclusionary rule jurisprudence. The Supreme Court has made clear that "suppression is not an automatic consequence of a Fourth Amendment violation," but instead "turns on the culpability of the police and the potential of exclusion to deter wrongful police misconduct." *Herring v. United States*, 555 U.S. 135, 137 (2009); *Illinois v. Gates*, 462 U.S. 213, 223 (1983) ("The fact that a Fourth Amendment violation occurred—i.e., that a search or arrest was unreasonable—does not necessarily mean that the exclusionary rule applies."). In *Herring*, the Supreme

Court refused to suppress evidence obtained from the warrantless search of the defendant's person and vehicle incident to his arrest pursuant to a non-existent arrest warrant. *Id.* at 147. The Court explained that, “[t]o trigger the exclusionary rule, police conduct must be sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system.” *Id.* at 144. The Court's emphasis on balancing deterrence and culpability in *Herring* did not mark a drastic departure from *United States v. Leon*, 468 U.S. 897, 922 (1984), where the Court stated that “the marginal or nonexistent benefits produced by suppressing evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion,” but it did signal the Court's shift “toward preserving evidence for use in obtaining convictions, even if illegally seized, than toward excluding evidence in order to deter police misconduct unless the officers engage in ‘deliberate, reckless, or grossly negligent conduct.’” *Master*, 614 F.3d at 243 (quoting *Herring*, 555 U.S. at 144). “Indeed, exclusion ‘has always been our last resort, not the first impulse,’ and our precedents establish important principles that constrain application of the exclusionary rule.” *Herring*, 555 U.S. at 140 (quoting *Hudson v. Michigan*, 547 U.S. 586, 591 (2006)).

*Herring* makes clear that this Court erred in holding that the good-faith exception does not apply to a search conducted pursuant to a warrant that is void at the outset. *Herring* involved the unlawful arrest of an individual pursuant to a warrant that had been rescinded five months earlier. 555 U.S. at 137-38. Although the arrest warrant had no legal force—essentially, it no longer existed—and thus did not authorize the defendant's arrest, the Supreme Court proceeded to consider whether the officers' reliance on the non-existent warrant was objectively reasonable in deter-

mining whether evidence obtained from the warrantless search incident to the unlawful arrest should be suppressed. *Id.* at 141-44. Thus, even if this Court adheres to its ruling that the NIT warrant, like the arrest warrant in *Herring*, was no warrant at all, *Herring* dictates that the suppression is not automatic, and that the officers' good faith—as well as the deterrent benefits of suppression—must be considered in deciding whether to invoke the exclusionary rule.

Moreover, assuming that the NIT Warrant is not void *ab initio*, which it is not for the reasons discussed above, the exclusionary rule is not an appropriate remedy because the agents relied on the now-invalidated warrant in good faith, and suppression provides no deterrent benefit. There is absolutely no evidence of deliberate, reckless, or grossly negligent conduct on behalf of the law enforcement agents who applied for the NIT warrant; to the contrary, the warrant application reflects the agents' best efforts to comply with Rule 41(b) by seeking approval for the NIT warrant in the judicial district where the NIT would be deployed from Playpen's server, with which the activating computers voluntarily communicated, and the information it retrieved from the activating computers would be received. Since the location of the activating computers was unknown at the time of NIT deployment, it was not unreasonable for the agents to conclude that the NIT deployment and receipt location into which activating computers were communicating—the Eastern District of Virginia—represented the strongest known connection to the criminal activity under investigation. That the agents' compliance efforts were subsequently found insufficient by this Court does not mean that it was objectively unreasonable for the agents to have believed that the NIT warrant was properly issued, especially "given that reasonable minds can differ as to the degree of Rule 41(b)'s flexibility in uncharted territory." *Michaud*, 2016 WL 337263, at \*7. *See also Massachusetts v. Sheppard*, 468

U.S. 981, 987-88 (1984) (stating that “the exclusionary rule should not be applied when the officer conducting the search acted in objectively reasonable reliance on a warrant issued by a detached and neutral magistrate,” even if that warrant “is subsequently determined to be invalid”).

Finally, the court must consider whether “the benefits of deterrence outweigh the costs.” *Herring*, 555 U.S. at 141. Suppression is an extreme remedy and the costs to society and the justice system of excluding evidence obtained from the NIT warrant—freeing defendants from prosecution for their crimes against children—are immense, yet suppression will have absolutely no deterrent effect on future police misconduct. On April 28, 2016, the Supreme Court approved an amendment to Rule 41(b) that clarifies the scope of a magistrate judge’s authority to issue warrants, such as the NIT warrant, to remotely search computers located within or outside the issuing district if the computer’s location has been concealed through technological means. Once this amendment becomes effective on December 1, 2016, the Rule 41(b) violation that the Court found to have occurred in this case will never occur again. Applying the exclusionary rule in this case will only punish law enforcement for a past mistake, not deter any future misconduct. *See Herring*, 555 U.S. at 141 (noting that the primary purpose of the exclusionary rule is “detering Fourth Amendment violations in the future”). Because the “nonexistent benefits produced by suppressing evidence obtained in objectively reasonable reliance on a subsequently invalidated search warrant cannot justify the substantial costs of exclusion,” *Leon*, 468 U.S. at 922, suppression is not warranted here.

**4. The facts of this case warrant an exigent-circumstances exception to the application of the exclusionary rule.**

The Supreme Court has recognized that the presumption that warrantless searches are unreasonable “may be overcome in some circumstances because [t]he

ultimate touchstone of the Fourth Amendment is ‘reasonableness.’” *Kentucky v. King*, 131 S. Ct. 1849, 1856 (2011) (quoting *Brigham City v. Stuart*, 547 U.S. 398, 403 (2006)). “One well-recognized exception applies when ‘the exigencies of the situation make the needs of law enforcement so compelling that [a] warrantless search is objectively reasonable under the Fourth Amendment.’” *Id.* (quoting *Mincey v. Arizona*, 437 U.S. 385, 394 (1978)). Courts must evaluate “the totality of the circumstances” to determine whether exigencies justified a warrantless search. *Missouri v. McNeely*, 133 S. Ct. 1552, 1559 (2013).

In the Tenth Circuit, the *Aquino* test sets forth four requirements for a permissible warrantless entry: (1) there is clear evidence of probable cause for the criminal violation, (2) the crime is a serious one and one in which the destruction of evidence (or other purpose that frustrates legitimate law enforcement efforts) is likely, (3) the entry is limited in scope to the minimum intrusion necessary to prevent the destruction of evidence (or other frustrating purpose), and (4) the exigency is supported by clearly defined indicators that are not subject to police manipulation or abuse. *United States v. Aguirre*, No. 16-CR-0027-CVE, 2016 WL 1464574, at \*11 (N.D. Okla. Apr. 14, 2016) (citing *United States v. Aquino*, 836 F.2d 1268, 1272 (10th Cir. 1988)).

Here, the four requirements are all satisfied. First, clear evidence of probable cause existed regarding the Tor-based child pornography trafficking investigation. “Probable cause to search requires ‘a fair probability that contraband or evidence of a crime will be found in a particular place.’” *United States v. Hendrix*, 664 F.3d 1334, 1338 (10th Cir. 2011) (quoting *United States v. Cooper*, 654 F.3d 1104, 1124 (10th Cir. 2011)). As discussed above and laid out more fully in the United States’ Response (Doc. 34), the NIT warrant contained sufficient probable cause in light of the identity



encryption on the Tor network, Playpen's "hidden service" status, Playpen's landing page, the terms of Playpen's registration, and the vast amounts of child pornography contained within the site.

Second, the trafficking of child pornography is an uncontroversially serious crime. Playpen enabled the ongoing sexual abuse and exploitation of children committed by unidentified offenders against unidentified children. Deploying the NIT against Playpen's users was necessary to stop the abuse and exploitation and to identify and apprehend the abusers, as well as identify and rescue those children. As of early January 2016, use of the NIT in the nationwide investigation of Playpen had led to the identification or recovery from abuse of at least 26 child victims. *See Michaud*, No. 15-CR-5351-RJB (Doc. 109 at 8). The FBI also has identified at least 35 individuals who have been determined to be "hands on" child sexual offenders, and at least 17 individuals who have been determined to be producers of child pornography. *Id.* at 7-8. And the circumstances of the online trafficking on the Tor network indicated that the destruction and loss of evidence was likely. The criminal activity of accessing with intent to view, receipt, and distribution of child pornography was carried out through the encrypted network. As noted in the search warrant application, traditional investigative techniques were either unsuccessful or reasonably unlikely to succeed due to the encryption. The transmittal of the contraband and evidence of the identity of the user was only available while the user was online and accessing the website. Once the user was logged off, the information was no longer being transmitted through the relay nodes and the evidence of what was being transmitted and who was transmitting it was not present for capture. To interdict the criminal activity and capture evidence of the offense, other than the steps taken by law enforcement here, it would have been impossible to obtain a warrant in time

to capture the activity. When users might access the site for a matter of minutes or hours, issuing generalized warrants in every district across the country is logistically impossible. *See, e.g., Cupp v. Murphy*, 412 U.S. 291, 296 (1973) (affirming use of warrantless search to prevent loss or destruction of “highly evanescent” evidence). Accordingly, the frustration of law enforcement efforts was likely under the circumstances of the defendant’s criminal conduct.

Third, as stated above, the search was minimally intrusive since it sought to capture only information—his IP address—that the defendant was readily utilizing through his Internet Service Provider (“ISP”) every time he connected to the Internet or Tor network. Importantly, the defendant’s IP address belonged to his ISP, not to him, and courts have held that a defendant lacks a reasonable expectation of privacy in his IP address. *See, e.g., United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2007); *Michaud*, 2016 WL 337263, at \*7 (lack of reasonable expectation of privacy does not change with the use of Tor); *United States v. Farrell*, No. CR15-029RAJ, 2016 WL 705197, at \*2 (W.D. Wash. Feb. 23, 2016) (same). Before proceeding with a more invasive entry and search of the defendant’s home and electronic devices, the government obtained a Rule 41 warrant issued in this district.

Finally, despite the court’s order, the exigency that existed was not subject to police manipulation or abuse. In suppressing the NIT warrant, the court rejects an argument on exigent circumstances stating “the specific activity at issue was on-going only because the Government opted to keep the Playpen site operation while it employed the NIT. The Government cannot assert exigent circumstances when it had a hand in creating the emergency.” Doc. 42 at 27. This assertion should be reconsidered in light of *Kentucky v. King*, specifically, law enforcement officers did not take any action that violated or threatened to violate the defendant’s Fourth

Amendment rights. *King*, 563 U.S. 452, 462 (2011) (“Where . . . the police did not create the exigency by engaging or threatening to engage in conduct that violates the Fourth Amendment, warrantless entry to prevent the destruction of evidence is reasonable and thus allowed.”). Here, the exigent circumstances are to prevent the on-going child pornography violations by capturing the perpetrators and the agents complied with the Fourth Amendment. Actions that do not rise to constitutional violations or threats to violate constitutional rights, such as continuing to run the Playpen site, are not relevant to the *King* analysis. Furthermore, there was nothing else the agents could have done to comply with the various rule and statutory restrictions on warrants.

When confronted with the activity on the Playpen site, agents became aware that traffickers in child pornography were utilizing anonymization software to come and go as they pleased on an illicit website, accruing and distributing untold amounts of contraband. In that moment, the exigency was clear and present. Those who downloaded or distributed child pornography prior to the instant the NIT was deployed were getting away with heinous offenses. Agents worked quickly to attempt to capture the fleeting evidence of the crime being committed and identity of the perpetrator. They sought, in good faith, a NIT that was judicially authorized and in compliance with the Fourth Amendment’s warrant requirements. As opposed to suppressing the evidence of the defendant’s criminal activity, this Court should reconsider and determine that exigent circumstances provide an exception to the exclusionary rule and that the subsequent search warrant in this district remain.

CONCLUSION

For the foregoing reasons, the United States respectfully requests that this Court reconsider its order granting the defendant's motion to suppress evidence obtained from the NIT warrant.

Respectfully submitted,

DANNY C. WILLIAMS, SR.  
United States Attorney

/s/ Andrew J. Hofland  
Andrew J. Hofland, WI Bar #1065503  
Assistant United States Attorney  
110 West Seventh Street, Suite 300  
Tulsa, Oklahoma 74119-1029  
(918) 382-2700  
andrew.hofland@usdoj.gov

**CERTIFICATE OF SERVICE**

I hereby certify that on the 13th day of June, 2016, I electronically transmitted the foregoing document to the Clerk of Court using the ECF System for sealed filing and transmittal of a Notice of Electronic Filing to the following ECF registrant:

William Widell  
*Counsel for Defendant*

/s/ Andrew J. Hofland  
Andrew J. Hofland  
Assistant United States Attorney

**IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
NORFOLK DIVISION**

**UNITED STATES OF AMERICA,**

**v.**

**CRIMINAL NO. 2:16cr36**

**GERALD ANDREW DARBY,**

**Defendant.**

**OPINION AND ORDER**

This matter comes before the Court on Two Motions to Suppress filed by Gerald Andrew Darby (“Defendant”). ECF Nos. 15, 18. For reasons set forth below, the Court **DENIES** Defendant’s First Motion to Suppress, ECF No. 15, and **DENIES** Defendant’s Second Motion to Suppress, ECF No. 18.

**I. BACKGROUND**

The instant prosecution is the result of an FBI investigation into a website that facilitated the distribution of child pornography. The government seized control of this website and for a brief period of time operated it from a government facility in the Eastern District of Virginia. Both Motions to Suppress seek to exclude all evidence obtained as the result of a search warrant that allowed the government to use the website to remotely search the computers of individuals who logged into the website.

The following summary is provided as way of background. There is not yet any evidentiary record in this case, but the basic details of the investigation are not in dispute. Most of the information summarized here has been drawn from the warrant application, Appl. for a Search Warrant (“Warrant Appl.”), ECF No. 16-1, specifically the affidavit in support of the warrant sworn to by FBI Special Agent Douglas Macfarlane. Aff. in Supp. of Appl. for Search

Warrant (“Aff., Warrant Appl.”), ECF No. 16-1 at 6. Additional details undisputed by the parties in their briefing are included mainly to fill out the narrative. For instance, neither the warrant nor warrant application identify the website and both refer to it simply as “TARGET WEBSITE.” See Aff., Warrant Appl., ¶ 4. As explained in the affidavit in support of the warrant, at the time the warrant application was submitted the website was still active. Id. ¶ 2 n.1. The government was concerned that disclosure of the name of the website in the application would alert potential users of the site to the government’s investigation and thus undermine it. Id. At present, the government has since ceased operation of the website, and the name of the website has been widely reported.<sup>1</sup> Both parties refer to the website by its name: Playpen.

Playpen operated on the Tor network, which provides more anonymity to its users than the regular Internet.<sup>2</sup> Aff., Warrant Appl., ¶¶ 7–8. The Tor network was developed by the U.S. Naval Research Laboratory and is now accessible to the general public. Id. ¶ 7. Users of the Tor network must download special software that lets them access the network. Id. Typically, when an individual visits a website, the website is able to determine the individual’s Internet Protocol (“IP”) address. See id. ¶ 8. An individual’s IP address is associated with a particular Internet Service Provider (“ISP”) and particular ISP customer. Id. ¶ 35. Because internet access is typically purchased for a single location, an IP address may be used by law enforcement to determine the home or business address of an internet user. See id. When a user accesses the Tor network, communications from that user are routed through a system of network computers that are run by volunteers around the world. Id. ¶ 8. When a user connects to a website, the only IP address that the website “sees” is the IP address of the last computer through which the user’s

---

<sup>1</sup> See e.g., Joseph Cox, The FBI’s ‘Unprecedented’ Hacking Campaign Targeted Over a Thousand Computers, Motherboard, Jan. 5, 2016, <http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers>.

<sup>2</sup> The Tor network is also known as “The Onion Router.” Aff., Warrant Appl., ¶ 7. More information about it may be found on its website: [www.torproject.org](http://www.torproject.org).

communications were routed. Id. This final relay is called an exit node. Id. Because there is no practical way to trace a user's communications from the exit node back to the user's computer, users of the Tor network are effectively anonymous to the websites they visit. Id.

The Tor network also provides anonymity to the individuals who run websites or forums on it. Id. ¶ 9. Websites may be set up on the Tor network as "hidden services." Id. A hidden service may only be accessed through the Tor network. Id. A hidden service functions much like a regular website except that its IP address is hidden. Id. The IP address is replaced with a Tor-based address which consists of a series of alphanumeric characters followed by ".onion." Id. There is no way to look up the IP address of the computer hosting a hidden service. Id.

A user of the Tor network cannot simply perform a search to find a hidden service that may interest the user. Id. ¶ 10. In order to access a hidden service a user must know the Tor-based address of the hidden service. Id. As a result, a user cannot simply stumble onto a hidden service. Id. The user may obtain the address from postings on the Internet or by communications with other users of the Tor network. Id. One hidden service may also link to another. See id. Playpen was a hidden service contained on the Tor network, and it had been linked to by another hidden service that was dedicated to child pornography. Id.

Of importance to the First Motion to Suppress is the homepage of the Playpen site. See Def.'s First Mot. to Suppress ("First Mot."), ECF No. 15 at 2–3. In the warrant application, the homepage is said to contain "images of prepubescent females partially clothed and whose legs are spread." Aff., Warrant Appl., ¶ 12. The censored version of the exact images has been attached to the briefing. ECF No. 16-2. There appears to have just been two photographs on the home page. The images show two young girls in the attire and pose described. Id. The images of these children appear at the top of the homepage and flank a large image of the site's name,

Playpen. Id. Although these images were at an earlier point on the homepage, the parties agree that at the time the warrant was signed, on February 20, 2015 at 11:45 am, a different image confronted users to the site. First Mot. at 9; Gov't's Resp. to Def.'s First Mot. to Suppress ("Gov't's Resp. to First Mot."), ECF No. 16 at 14. A censored version of this image has also been included in the briefing. ECF No. 16-3. It shows a young girl with her legs crossed, reclined on a chair, wearing stockings that stop at her upper thigh and a short dress or top that exposes the portion of her upper thigh not covered by the stockings. Id. Her image is to the left of the site name. Id.

The government claims that the images must have changed shortly before the warrant was signed. Gov't's Resp. to First Mot. at 14. In the affidavit in support of the warrant, Special Agent Macfarlane recounts that FBI agents reviewed the Playpen website from September 16, 2014 to February 3, 2015. Aff., Warrant Appl., ¶ 11. The screenshot of the home page that was included in the government's brief and contains the images of the two young girls was taken on February 3, 2015. ECF No. 16-2. The date is visible in the lower right corner of the screen. Id. The affidavit further states that sometime between February 3, 2015 and February 18, 2015, the Tor address of the site was changed. Warrant Appl. ¶ 11 n.1. Special Agent Macfarlane states in his affidavit that after the address change he "accessed the TARGET WEBSITE in an undercover capacity at its new URL, and determined that its content had not changed." Id. In its briefing the government asserts that this statement confirms that the homepage of Playpen was as described in the warrant application on February 18, 2015, two days before the warrant was sworn and signed. Gov't's Resp. to First Mot. at 14–15.

The homepage also provided users with instructions on how to join and then log into the site. Aff., Warrant Appl., ¶ 12. Users had to register with the site before going any further into



the site. Id. Users were instructed to enter a phony email address and to create a login name and password. Id. ¶ 13. The instructions also informed users that staff and owners of the site were unable to determine the true identity of users and that the website could not see the IP addresses of users. Id.

Once registered and logged into the site users had access to numerous sections, forums, and sub-forums where they could upload material and view material uploaded by others. Id. ¶14. For instance under the heading “Playpen Chan”<sup>3</sup> are four subcategories: “Jailbait – Boy,” “Jailbait – Girl,” “Preteen – Boy,” and “Preteen – Girl.” Id. Special Agent Macfarlane, based on his training and experience, explains that “jailbait” refers to underage but post-pubescent minors. Id. ¶ 14 n.4. Other forum and sub-forum categories on the site include “Jailbait videos,” “Family Playpen – Incest,” “Toddlers,” and “Bondage.” Id. ¶ 14. Not surprisingly, a review of the contents of these forums revealed that the majority of content was child pornography. Id. ¶ 18. The warrant application has several specific examples of the reprehensible material contained on the site. Id. ¶¶ 18, 23–25. Additionally, there was a section of the site that allowed members of the site to exchange usernames on a Tor-based instant messaging service known to law enforcement to be “used by subjects engaged in the online sexual exploitation of children.” Id. ¶ 15.

In December of 2014, a foreign law enforcement agency informed the FBI that it suspected that a United States-based IP address was the IP address of Playpen. Id. ¶ 28. In January 2015, after obtaining a search warrant, the FBI seized the IP address and copied the contents of the website. Id. ¶ 28. On February 19, 2015 the FBI arrested the individual suspected of administering Playpen. Id. ¶ 30.

---

<sup>3</sup> “Chan” is a common postscript for online bulletin boards where users may post pictures and messages. See Nick Bilton, One on One: Christopher Poole, Founder of 4chan, Bits Blog, New York Times, Mar. 19, 2010, <http://bits.blogs.nytimes.com/2010/03/19/one-on-one-christopher-poole-founder-of-4chan/>.

The FBI desired to continue to operate Playpen for a limited time so as to identify individuals who logged into the site and who were likely to possess, distribute, or produce child pornography. Id. ¶ 30. The FBI would operate the site from a location in the Eastern District of Virginia. Id. ¶ 33. As mentioned above, normally a website administrator is able to determine the IP addresses of those individuals that visit the site. However, on the Tor network the website administrator is only able to determine the IP address of the exit node, which is not the IP address of the visitor to the website. To determine the IP addresses of individuals who logged into Playpen, the FBI sought a warrant from a magistrate judge in the Eastern District of Virginia, Alexandria division, that would allow it to deploy a Network Investigative Technique (“NIT”). Id. ¶ 31.

According to the FBI in its warrant application, when an individual visits a website the website sends “content” to the individual. Id. ¶ 33. This content is downloaded by the individual’s computer and used to display the webpage on the computer. Id. A NIT “augments” the content with additional instructions. Id. The NIT deployed in the instant case instructed the computers of those individuals who logged into Playpen to send to a computer “controlled by or known to the government” certain information. Id. The information that the NIT would instruct the computers to send is described in an attachment to the warrant application. Attach. B, Warrant Appl., ECF No. 16-1 at 5. The NIT extracted from any “activating computer”—a computer that logged into Playpen using a username and password—(1) the IP address of the computer and the date and time this information is determined, (2) a unique identifier that distinguishes the data from this activating computer from that of others, (3) the type of operating system used by the computer, (4) information about whether the NIT has already been sent to the computer, (5) the computer’s Host Name, (6) the computer’s operating system user name, and

(7) the computer's media access control ("MAC") address. Id.

On February 20, 2016 at 11:45 am, Magistrate Judge Theresa Carroll Buchanan of the United States District Court for the Eastern District of Virginia, Alexandria Division, issued the requested warrant. Warrant Appl., ECF No. 16-1 at 39. The warrant permitted the FBI to run Playpen from a location in the Eastern District of Virginia for thirty (30) days and to deploy a NIT from the website. Id. at 37–39. The NIT would instruct any computer that logged into Playpen with a username and password to send the just described information. Id. at 37–38.

According to the briefing of the defendant, Gerald Andrew Darby ("Defendant"), on or about February 27, 2015, the NIT on the Playpen website sent instructions to Defendant's computer.<sup>4</sup> First Mot. at 10. The FBI identified Defendant's IP address and issued an administrative subpoena to his ISP, Verizon. Id. at 10–11. Verizon provided Defendant's name, subscriber information, and address to the government. Id. On January 4, 2016, a warrant to search Defendant's home was issued by Magistrate Judge Robert J. Krask. Id. at 11. FBI agents searched Defendant's home on January 7, 2016 and seized computers, hard drives, cell phones, tablets, video game systems, and other property. Id. According to the government, Defendant was present during the search and agreed to be interviewed. Gov't's Resp. to First Mot. at 7. During this interview Defendant admitted to downloading sexually explicit images of minors for the past three to four years. Id. The government also relates that forensic analysis found that Defendant possessed 1,608 images and 298 videos of child pornography. Id.

On March 10, 2016 a grand jury returned an indictment charging Defendant with five counts of Receipt of Images of Minors Engaging in Sexually Explicit Conduct in violation of 18 U.S.C. § 2252(a)(2) and three counts of Possession of Images of Minors Engaging in Sexually

---

<sup>4</sup> Defendant identifies his Playpen username as "Broden" while the government identifies the username as "NeoUmbrella." First Mot. at 10; Gov't's Resp. to First Mot. at 16. This apparent disagreement does not affect any of the analysis in this case.

Explicit Conduct in violation of 18 U.S.C. § 2252(a)(4)(B). ECF No. 1. Defendant filed his First Motion to Suppress on April 13, 2016. ECF No. 15. The government filed its Response in Opposition on April 27, 2016. ECF No. 16. Defendant filed his Second Motion to Suppress on May 3, 2016, and the government responded to this motion of May 9, 2016. ECF Nos. 18, 22. A hearing on both motions was held on May 10, 2016. Hr'g, ECF No. 24.

## **II. DEFENDANT'S MOTIONS TO SUPPRESS**

Both of Defendant's Motions to Suppress challenge the warrant, issued by Magistrate Judge Theresa Buchanan, which authorized the deployment of the NIT through the government's administration of the Playpen website. Because the second warrant, which authorized the search of Defendant's home, was issued on account of information gathered pursuant to the NIT Warrant, Defendant seeks to suppress all evidence obtained during the search of his home.

### **A. WAS DEPLOYMENT OF THE NIT A FOURTH AMENDMENT SEARCH?**

Before reaching the merits of Defendant's motions, it will be useful to address a preliminary question unaddressed by the parties: Was the deployment of the NIT a "search" of Defendant's computer within the meaning of the Fourth Amendment? If the use of the NIT was not a search, the Fourth Amendment was not implicated, no warrant was required, and any violation of Rule 41(b) irrelevant. See *Kyllo v. United States*, 533 U.S. 27, 31 (2001) (referring to the "antecedent question whether or not a Fourth Amendment 'search' has occurred").

The government in its response to Defendant's First Motion to Suppress never argues that no warrant was required because deployment of the NIT was not a Fourth Amendment search. See Gov't's Resp. to First Mot. at 15–38. In failing to raise this argument when it would have been appropriate, the government has likely waived it. The government does, in justifying the scope of the warrant, argue that Defendant had no reasonable expectation of privacy in his IP address, even though he was using the Tor network. Id. at 33–34. However, the government

never pushes this point to its possible conclusion: that the use of the NIT was not a Fourth Amendment search because Defendant had no expectation of privacy in the information obtained by the NIT. Similarly, the government, in a recent filing, has drawn the Court's attention to a recent case from the Eastern District of Pennsylvania, United States v. Werdene, No. 2:15-cr-434-GJP, ECF No. 33 (E.D. Pa. May 18, 2016). In Werdene, the district court discussed whether the alleged Rule 41(b) violation was constitutional or procedural, a distinction that will be explained below. Id. at 14–20. In determining that the violation was not constitutional, the district court held that users of the Tor network have no reasonable expectation of privacy in their IP addresses. Id. However, the district court did not—perhaps because not urged to by the government—hold that because Tor users had no reasonable expectation of privacy in their IP address, no warrant was necessary to deploy the NIT and therefore any violation of rule 41(b) irrelevant. See id.

It will be instructive to explore fully whether the deployment of the NIT was a Fourth Amendment search. In deciding this question the Court will have to analyze just how a NIT works. Doing so will elucidate the privacy concerns raised by the NIT and clarify what is and is not at stake in this case. The discussion will also aid the analysis below concerning a possible violation of Rule 41(b).

A Fourth Amendment search occurs when “the person invoking its protection can claim a ‘justifiable,’ a ‘reasonable,’ or a ‘legitimate expectation of privacy’ that has been invaded by government action.” Smith v. Maryland, 442 U.S. 735, 740 (1979) (collecting cases). The classic analysis of this rule comes from Justice Harlan, who explained that there are two components to a reasonable expectation of privacy: “first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to

recognize as ‘reasonable.’” Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). In more recent years the Supreme Court has recognized, or reiterated, that a search may also occur when the government trespasses upon the areas—“persons, houses, papers, and effects”—enumerated in the Fourth Amendment. United States v. Jones, 132 S. Ct. 945, 950 (2012).

The government contends that Defendant had no reasonable expectation of privacy in his IP address even though he was using the Tor network, which is designed to shield the IP addresses of its users. The government does not address whether Defendant had a reasonable expectation of privacy in the other information gathered by the NIT, such as the type of operating system on Defendant’s computer and his computer’s Host name. But this piecemeal analysis of what this NIT was authorized to extract from Defendant’s computer misses the mark. The NIT surreptitiously placed code on Defendant’s personal computer that then extracted from the computer certain information. See Aff., Warrant Appl., ¶ 33. In placing code on Defendant’s computer, the NIT gave the government access to the complete contents of Defendant’s computer. The relevant inquiry is whether Defendant has a reasonable expectation of privacy in the contents of his personal computer, which was located in his home.

Several Courts of Appeals, including the Fourth Circuit, have held that individuals generally have a reasonable expectation of privacy in the contents of their home computers. Trulock v. Freeh, 275 F.3d 391, 403 (4th Cir. 2001); United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004); Guest v. Leis, 255 F.3d 325, 333 (6th Cir. 2001). Individuals’ subjective expectation of privacy in their computers is apparent from the mass of personal and financial information often contained on computers. This widespread practice is also evidence that society is prepared accept this subjective expectation of privacy. To be sure, personal computers are

vulnerable to hacking when connected to the internet, just as homes are vulnerable to break-ins. This criminality is not enough to defeat an individual's reasonable expectation of privacy. The prohibition against hacking is itself proof of society's acceptance of the privacy expectations of personal computer users. See 18 U.S.C. § 1030(a)(2)(C).

A recent Supreme Court case supports considering whether Defendant had a reasonable expectation of privacy in the contents of his computer rather than in the specific information the NIT commanded the computer to transmit. In Riley v. California, the Court considered “whether the police may, without a warrant, search digital information on a cell phone seized from an individual who has been arrested.” 134 S. Ct. 2473, 2480 (2014). The Court held that the police generally may not.<sup>5</sup> Id. at 2485. The Court rejected a suggestion by the United States that police could at the very least access the call records contained in an arrestee's cell phone. Id. at 2492–93. The United States had pointed out that the Court had held in Smith v. Maryland that individuals do not have a reasonable expectation of privacy in the phone numbers they dial. 442 U.S. 735, 745 (1979). There was no reasonable expectation of privacy because individuals voluntarily convey the numbers they dial to the phone company. Id. at 742–44. The Court in Riley distinguished Smith by noting that the ultimate holding in Smith was that the government's use of a pen register in that case was not a search under the Fourth Amendment. Riley, 134 S. Ct. at 2492. A pen register is a limited technology that can only record the phone numbers dialed by an individual. Smith, 442 U.S. at 740–41. By contrast, the Court in Riley said that it was undisputed that accessing the information in an individual's cell phone is a search. 134 S.Ct. at 2492–93. It was irrelevant that the individual might not have a reasonable expectation of privacy in the information actually obtained. See id.

---

<sup>5</sup> In so holding the Court emphasized the extensive amount of personal information typically held on modern cell phones. Id. at 2491. Personal computers of course typically contain a similar mass of personal information.

Likewise, if an individual has a reasonable expectation of privacy in the contents of his or her personal computer, as he or she does, and the deployment of the NIT invades that privacy, then the NIT is a search. The NIT in this case caused Defendant's computer to download certain code without the authorization or knowledge of Defendant. The "contents" of a computer are nothing but its code. In placing code on Defendant's computer, the government literally—one writes code—invaded the contents of the computer. Additionally, the code placed on Defendant's computer caused Defendant's computer to transmit certain information without the authority or knowledge of Defendant. In this manner the government seized the contents of Defendant's computer. Just as in Riley, it is irrelevant that Defendant might not have a reasonable expectation of privacy in some of the information searched and seized by the government. The government's deployment of the NIT was a Fourth Amendment search.

#### **B. DEFENDANT'S FIRST MOTION TO SUPPRESS**

In his First Motion to Suppress Defendant raises several related grounds for suppressing the fruits of the search executed pursuant to the NIT Warrant. First, he argues that the warrant was not supported by probable cause. First Mot. at 2. Second, he argues the FBI, either intentionally or recklessly, misled the warrant issuing court with its description of Playpen's homepage and demands a Franks hearing on this issue. Id. at 2–3; see Franks v. Delaware, 438 U.S. 154 (1978). Third, he argues that the NIT Warrant was an anticipatory warrant and that the triggering event establishing probable cause did not occur. First Mot. at 3.

##### **1. Legal Principles**

The Fourth Amendment requires that searches and seizures be reasonable. Riley, 134 S. at 2482 (citing Brigham City v. Stuart, 547 U.S. 398, 403 (2006)). Generally, the reasonableness requirement of the Fourth Amendment requires that law enforcement obtain a judicial warrant before performing a search or seizure. Id. (citing Vernonia School Dist. 47J v. Acton, 515 U.S.



646, 653 (1995)). An application for a search warrant must provide a basis for a magistrate to find that there is probable cause for a search. See United States v. Gary, 528 F.3d 324, 328 (4th Cir. 2008). There is probable cause for a search when “the known facts and circumstances are sufficient to warrant a man of reasonable prudence in the belief that contraband or evidence of a crime will be found.” Ornelas v. United States, 517 U.S. 690, 696 (1996). This standard “is a ‘practical, nontechnical conception.’” Illinois v. Gates, 462 U.S. 213, 231 (1983) (quoting Brinegar v. United States, 338 U.S. 160, 176 (1949)). It depends on the considerations of everyday life which inform the decisions of reasonable and prudent men and women. Id.

Probable cause does not require that there be an “absolute certainty” that evidence of a crime will be found. Gary, 528 F.3d at 327. Rather, it requires that there is a “fair probability” that such evidence will be found. Gates, 462 U.S. at 238. Because “[r]easonable minds frequently may differ on the question whether a particular affidavit establishes probable cause” the Supreme Court has instructed district courts to accord “‘great deference’ to a magistrate’s determination” of probable cause. United States v. Leon, 468 U.S. 897, 914 (1984) (citing Spinelli v. United States, 393 U.S. 410, 419 (1969)). A reviewing court does not perform a *de novo* review of the magistrate’s finding of probable cause but only determines whether there was substantial evidence in the record in support of the magistrate’s finding. Massachusetts v. Upton, 466 U.S. 727, 728 (1984) (*per curiam*).

## 2. Analysis

The warrant allowed the government to place the NIT on the computers of anyone who registered and logged into the site. The legal analysis of each of Defendant’s three grounds for suppression ultimately turns on a single issue: Were those individuals who registered and logged into the website aware that the site contained child pornography? If they were, their computers likely contained child pornography and a search of their computers supported by probable cause.

Defendant argues that some individuals might have “innocently” logged into the site in the hope of finding legal—though perhaps repugnant—content such as nude photographs of children that do not qualify as pornography or pornography involving teenagers that have reached the age of majority. See First Mot. at 10 (mentioning legal child erotica); 12 (noting that all depictions of naked children are not pornography); 17 (discussing the repugnant but legal content available on the internet). Because not all of those who registered with the website would have been seeking child pornography, Defendant argues that the warrant was not supported by probable cause. As will be explained below, Defendant’s other grounds for suppression in his First Motion to Suppress depend upon this central contention.

In arguing that there was no probable cause, Defendant places a great deal of emphasis on the difference between the homepage of Playpen as described in the warrant and as it existed when the warrant was executed. First Mot. at 13. It is undisputed that when the warrant was executed the image on the top of the homepage by the site’s name was different than the two images described in the warrant application. The warrant application describes images of two prepubescent girls, on each side of the site name, with their underwear exposed and their legs spread. The homepage when the warrant was executed contained a single image, to the left of the site name, of a possibly older child with her legs crossed. According to Defendant, it was critical for the finding of probable cause that the Playpen homepage “displayed ‘partially clothed prepubescent females with their legs spread apart.’” First Mot. at 13 (citing Aff., Warrant Appl., ¶ 12).

At the outset the Court must reject Defendant’s contention that the image of the single child was innocuous because she is “fully clothed” and possibly over eighteen. First Mot. at 9. The child is obviously under eighteen and not at all fully dressed. She is wearing a short top or

dress and posed provocatively with her upper thigh exposed. ECF No. 16-3. It is unclear whether her dress or top is capable of reaching below the line of her stockings. Nevertheless her outfit is inappropriate for her age and strongly suggestive. To the extent one can or should differentiate among sexualized depictions of children, the images of the two girls that were previously on the homepage are more reprehensible. But that distinction does not subtract from the sexualized nature of the single image of child erotica that appeared on the homepage during the period in which the government operated Playpen. Either version of the homepage supports a finding of probable cause.

From the homepage, users could access a page that let them register for the site. Aff., Warrant Appl., ¶ 13. Users were then prompted with a message that informed them that the site administrators would be unable to identify registered visitors to the site. Id. This promise of anonymity alone did not establish probable cause to search the computers of those who visited the site. However, it does support the magistrate judge's determination that there was probable cause. Those looking for illegal content would be encouraged by this promise while those believing that the site contained legal material may have been warned of the reprehensible content within.

Furthermore, the homepage and logon process of Playpen are not the only basis for finding that the warrant was supported by probable cause. The warrant application contains detailed information about the illegal content available on the Playpen website. Aff., Warrant Appl., ¶¶ 14–27. Whatever legal content may have been available there, the abundance of child pornography available more than establishes probable cause to search the computers of visitors who knew about the site's contents. The warrant application asserts that, because sites on the Tor network are not searchable with the same ease that sites on the traditional internet are, most

visitors to Playpen must have been told of site's online address and knew of the content of the site before registering. Id. ¶ 10. Defendant refutes this and identifies both a search engine and index of sites on the Tor network. First Mot. at 16. Defendant claims that one could find Playpen when searching for sites containing sexually explicit content that was not child pornography. Id. The government counters by noting that the search engine identified by Defendant filters out sites containing child abuse. Gov't's Resp. to First Mot. at 18. Additionally, the warrant application notes that the address for Playpen was listed in a directory contain on another Tor hidden service that was dedicated to child pornography. Aff., Warrant Appl., ¶ 10.

Ultimately, no matter how searchable the Tor network may be, the magistrate judge would have been justified in concluding that those individuals who registered and logged into Playpen had knowledge of its illegal content. The Tor network itself, although it has legitimate uses, is an obvious refuge for those in search of illegal material. At the very least, the Tor network is less searchable than the regular Internet. Defendant fails to explain why someone would go to the trouble of entering the Tor network, locating Playpen, registering for the site, and then logging into the site if they were not looking for illegal content. It is not as if the Internet is not saturated in legal pornography. The magistrate's common sense judgment would justify her finding that an individual would likely only take these steps if he was seeking child pornography and knew he could find it on Playpen.

In sum, the information in the affidavit provided substantial evidence in support of the magistrate's finding that there was probable cause to issue the NIT Warrant. The homepage of the website was suggestive of its content and promised anonymity to registrants. Because the website itself was difficult to find, those who accessed it likely knew of its contents. Although it is not beyond possibility that some of those who logged into Playpen did so without intention of

finding child pornography, probable cause requires a fair probability that a search will uncover evidence, not absolute certainty.

Each of Defendant's other grounds for suppression are also without merit, primarily because there was probable cause to issue the NIT Warrant. Defendant asserts that the warrant was overbroad because it authorized searches of every individual that logged into Playpen, potentially "tens of thousands of computers." First Mot. at 23. This argument is curious. As explained above, there was probable cause to search the computers of individuals that logged into Playpen even though some of them might not have been seeking child pornography. The fact that Playpen facilitated rampant criminality does not affect this finding. Defendant compares the NIT Warrant to the general warrants—issued by the English judges against the colonists—that motivated the passage of the Fourth Amendment. See Virginia v. Moore, 553 U.S. 164, 169 (2008) (summarizing the motivations behind the passage of the Fourth Amendment). Comparing this warrant to those outrages trivializes the struggles of the American Revolution and the achievements of the Constitution. The NIT Warrant describes particular places to be searched—computers that have logged into Playpen—for which there was probable cause to search. It is not a general warrant.

Defendant also requests the Franks hearing based on the change to the Playpen homepage described above. First Mot. at 19–22. In Franks v. Delaware the Supreme Court established two prerequisites that must be satisfied before a defendant is entitled to a hearing on any inaccuracies in an affidavit in support of a warrant application. 438 U.S. at 155–56. A Franks hearing is required if (1) "the defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit," and (2) "the allegedly false statement is necessary to the finding of

probable cause” Id. At the hearing if, by a preponderance of evidence, the defendant establishes that the allegedly false statement was made knowingly or with reckless disregard of the truth, and, “with the affidavit’s false material set to one side, the affidavit’s remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit.” Id. at 156.

Neither of the requirements for a Franks hearing is met in this case. Defendant has failed to make a substantial preliminary showing that the inaccuracies regarding the Playpen homepage were made knowingly or with reckless disregard for the truth. The government took over Playpen on February 19, 2015. Aff., Warrant Appl., ¶ 30. The warrant was signed and executed on February 20, 2015. Warrant Appl. at 39. As discussed in the Background section above, the homepage certainly existed as described in the affidavit on February 3, 2015. The government took a screenshot of the page on that day and has attached it to its briefing. ECF No. 16-2. Additionally, Special Agent Macfarlane accessed the site on February 18, 2015 and found that it had not changed since February 3, 2015. Aff., Warrant Appl., ¶ 3 n.3. Based on the evidence before the Court, the website must have changed between February 18, 2015 and February 19, 2015. There is nothing reckless about relying on a visit to the website on February 18, 2015 when describing the website for a warrant signed and executed on February 20, 2015. Defendant has submitted no evidence that the government knew the site had changed. He merely makes conclusory allegations that the government must have known because they took over the site. First Mot. at 20. This is not enough to entitle Defendant to a Franks hearing.

Additionally, a Franks hearing is not justified because the alleged falsity in the affidavit was not necessary to the finding of probable cause. See United States v. Colkley, 899 F.2d 297,

300 (4th Cir. 1990) (“[T]o be material under Franks, an omission must do more than potentially affect the probable cause determination.”). As discussed, contrary to the repeated emphasis of Defendant, the images of two prepubescent females described in the warrant application were not necessary to the finding of probable cause. There was an abundance of other evidence before the magistrate judge that supported her finding that there was probable cause to issue the warrant.

Defendant also argues that the warrant was an anticipatory warrant whereby probable cause was established when a user logged into the homepage as described in the warrant application. First Mot. at 25–27. Because the homepage had changed, Defendant argues that this triggering event never occurred. Defendant’s argument is again premised on his contention that the images of two prepubescent females were necessary to the finding of probable cause. If probable cause only existed to search the computers of those that registered and logged into Playpen when it contained those images, then the triggering event of the warrant would not have occurred because those images were not on the webpage while the government operated it. However, as discussed, Defendant mischaracterizes the evidence before the magistrate judge in support of her finding of probable cause. Even without those images there was probable cause to search anyone who registered and logged into Playpen. Logging into Playpen was the triggering event, and all the computers searched under the NIT Warrant, including Defendant’s, logged into the site.

Because each of the grounds for suppression asserted in Defendant’s First Motion to Suppress is without merit, the Court **DENIES** Defendant’s First Motion to Suppress. ECF No. 15.

### **C. DEFENDANT’S SECOND MOTION TO SUPPRESS**

In his Second Motion to Suppress Defendant argues that the magistrate judge lacked jurisdiction under the Federal Magistrates Act, which incorporates Federal Rule of Criminal

Procedure 41(b), to issue the NIT Warrant. Def.'s Second Mot. to Suppress ("Second Mot."), ECF No. 18 at 2. Because the magistrate judge lacked jurisdiction to issue the warrant, the warrant was issued without lawful authority and void at the outset or *ab initio* in Latin. Id. If the warrant was void, the search of Defendant's computer was performed without a valid warrant in violation of the Fourth Amendment to the Constitution. Because of this alleged constitutional violation Defendant seeks to suppress all fruits of the search performed under the NIT Warrant. In the alternative, Defendant argues that the fruits of the NIT Warrant should be suppressed because he was prejudiced by the alleged violation of Rule 41(b) and because the government's violation of the rule was deliberate. Id.

### 1. Legal Principles

The Federal Magistrates Act in relevant part provides that

(a) Each United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law--

(1) all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts;

28 U.S.C. § 636(a). Rule 41(b) of the Federal Rules of Criminal Procedure, which are explicitly incorporated by the Federal Magistrates Act in above text, provides

(b) Authority to Issue a Warrant. At the request of a federal law enforcement officer or an attorney for the government:

(1) a magistrate judge with authority in the district -- or if none is reasonably available, a judge of a state court of record in the district -- has authority to issue a warrant to search for and seize a person or property located within the district;

(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;

(3) a magistrate judge--in an investigation of domestic terrorism or international terrorism--with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant



- for a person or property within or outside that district;
- (4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and
- (5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:
- (A) a United States territory, possession, or commonwealth;
  - (B) the premises--no matter who owns them--of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission's purposes; or
  - (C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

There are two types of Rule 41 violations: those that involve the constitutional violations and those that do not. United States v. Simons, 206 F.3d 392, 403 (4th Cir. 2000). Suppression is warranted for non-constitutional violations of Rule 41 “only when the defendant is prejudiced by the violation or when there is evidence of intentional and deliberate disregard of a provision in the Rule.” Id. (internal citations and quotations omitted).

## 2. Analysis

Defendant’s basic argument is simple: nothing in Rule 41(b) allowed the magistrate judge to issue the NIT Warrant. The NIT Warrant allowed the government to utilize the NIT against any computer that logged into the Playpen website. These computers could have been located anywhere in the world. Defendant argues that Rule 41(b) only allows magistrate judges to issue warrants for searches outside of their districts in limited, well-defined circumstances, none of which apply to the facts of the instant case. Second Mot. at 6–11. Of course, Defendant acknowledges that the website was being run from within the Eastern District of Virginia, that the magistrate judge sits in the Eastern District of Virginia, and that Defendant’s computer was located in the Eastern District of Virginia when the NIT was deployed. However, according to

Defendant, it is irrelevant that magistrate judge could have issued a warrant to search his computer because the warrant was not limited to him or the Eastern District of Virginia. See Second Mot. at 16.

It is understandable why the government sought the warrant in the Eastern District of Virginia. The government planned to run the website from a server located in the district. No district in the country had a stronger connection to the proposed search than this district. Additionally, nothing in Rule 41 categorically forbids magistrates from issuing warrants that authorize searches in other districts—most of its provisions do just that. See Fed. R. Crim. P. 41(b)(2–5). In its briefing the government notes that the Supreme Court has authorized an amendment to Rule 41(b)—to be effective December 1, 2016 absent action from Congress—that explicitly authorizes warrants like the NIT Warrant to be issued by magistrate judges whose districts have a connection with the criminal activity being investigated.<sup>6</sup> Gov’t’s Resp. to Def.’s Second Mot. to Suppress (“Gov’t’s Resp. to Second Mot.”), ECF No. 22 at 6; see also ECF No. 22-1, Ex. 1 (a copy of the amendment submitted to congress). The government characterizes this amendment as clarifying the scope of Rule 41(b), and this Court agrees.

In other words, as currently written Rule 41(b) gave the magistrate judge authority to issue the NIT Warrant. Rule 41(b)(4) allows a magistrate judge to issue a warrant for a tracking device to be installed in the magistrate’s district. Once installed, the tracking device may continue to operate even if the object tracked moves outside the district. This is exactly analogous to what the NIT Warrant authorized. Users of Playpen digitally touched down in the

---

<sup>6</sup> The proposed addition to the rule reads in relevant part “a magistrate judge with authority in any district where activities related to a crime may have occurred has authority 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: (A) the district where the media or information is located has been concealed through technological means . . . .” Fed. R. Crim. P. 41(b)(6) (proposed amendment).

Eastern District of Virginia when they logged into the site. When they logged in, the government placed code on their home computers. Then their home computers, which may have been outside of the district, sent information to the government about their location. The magistrate judge did not violate Rule 41(b) in issuing the NIT Warrant.<sup>7</sup>

But even if there were a Rule 41(b) violation, suppression would not be appropriate. Defendant seeks suppression on two related theories. Defendant argues for suppression solely on account of the violation of Rule 41(b) even if it was not of constitutional character. Suppression is warranted for a non-constitutional violation of Rule 41 only if the violation is intentional and deliberate or if the defendant seeking suppression is prejudiced by the violation. Defendant argues that the violation was deliberate because the Department of Justice has been trying to amend Rule 41(b) to allow explicitly this type of warrant. Therefore, Defendant argues, the federal agents knew that the NIT Warrant was not authorized by Rule 41(b). In other words, Defendant seeks to attribute to the FBI agents that sought the warrant the legal expertise of the DOJ lawyers, which is absurd. As discussed above, it was quite logical for the FBI to seek this warrant in the Eastern District of Virginia. Even if this Court is incorrect in holding that there was no violation of Rule 41(b), there is a credible argument that the current rule allowed this warrant. Additionally, it is hard to fathom why the FBI would go through the trouble of seeking a warrant in deliberate violation of Rule 41(b). If they were so inclined to undermine individual rights, they might have forgone seeking the warrant in the first place. But they tried to comply with the Fourth Amendment and the Federal Rules of Criminal Procedure. Any violation of Rule 41(b) was unintentional.

---

<sup>7</sup> The government also argues that Rule 41(b)(2) allows the NIT Warrant. Gov't's Resp. to Second Mot. at 3–4. However this Rule only allows a magistrate judge to issue a warrant to search “a person or property outside the district if the person or property is located within the district when the warrant is issued.” Fed. R. Crim. P. 41(b)(2). At the time the warrant was issued, Defendant’s computer was outside the district and not accessing the website.

Nor has Defendant been prejudiced by any Rule 41(b) violation. Defendant's computer was in the Eastern District of Virginia when the warrant was executed. Rule 41(b) of course allows magistrate judges to issue warrants authorizing searches of persons and property in their judicial district. Fed. R. Crim. P. 41(b)(1). In more strictly delineating the instances in which magistrate judges may issue warrants for searches outside their district, the Rule protects individuals from being subjected to the powers of distant governmental officials. See United States v. Krueger, 809 F.3d 1109, 1125 (10th Cir. 2015) (Gorsuch, J., concurring) (“[O]ur whole legal system is predicated on the notion that good borders make for good government, that dividing government into separate pieces bounded both in their powers and geographic reach is of irreplaceable value when it comes to securing the liberty of the people.”). This Defendant was not subject to the power of a distant official, and so was not prejudiced by any violation of Rule 41(b).

As mentioned at the outset of this section, Defendant also seeks suppression on constitutional grounds. He argues that Section 636(a) of the Federal Magistrates Act limits the jurisdiction of magistrates to issue search warrants and that this jurisdiction is defined by Rule 41(b). Because, according to Defendant, the NIT Warrant was issued in violation of Rule 41(b), it was void at its issuance. Therefore, the search of Defendant's computer was allegedly performed without a warrant in violation of the Fourth Amendment to the Constitution.

Of course, not all Fourth Amendment violations require the suppression of the evidence seized as a result.<sup>8</sup> As the Supreme Court has emphasized, “[e]ach time the exclusionary rule is

---

<sup>8</sup> In addition to the good faith exception discussed here, the government makes two additional arguments for why suppression is not warranted. The government argues that even if the NIT Warrant was void, a warrantless search was justified by exigent circumstance. Gov't's Resp. to Second Mot. at 9-11; see Kentucky v. King, 563 U.S. 452, 460 (2011). Of course, the government was able to obtain a warrant in this case, somewhat undercutting this

applied it exacts a substantial social cost for the vindication of Fourth Amendment rights.” Rakas v. Illinois, 439 U.S. 128, 137 (1978). The exclusionary rule should only be applied when its benefits outweigh its costs. Herring v. United States, 555 U.S. 135, 141 (2009). In furtherance of this principle, the Supreme Court has established a so-called “good faith” exception to suppression. See id. at 142. “When police act under a warrant that is invalid for lack of probable cause, the exclusionary rule does not apply if the police acted ‘in objectively reasonable reliance’ on the subsequently invalidated search warrant.” Id. (quoting United States v. Leon, 468 U.S. 897, 922 (1984)).

Behind this exception is the recognition that the purpose of the exclusionary rule is to deter unlawful police conduct. United States v. Gary, 528 F.3d 324, 329–30 (4th Cir. 2008) (citing Leon, 468 U.S. at 918). Accordingly, the Court has instructed district courts to consider whether the conduct of law enforcement was: (1) “sufficiently deliberate [such] that exclusion can meaningfully deter it,” and (2) “sufficiently culpable that such deterrence is worth the price paid by the justice system.” Id. at 144.

The FBI agents in this case did the right thing. They gathered evidence over an extended period and filed a detailed affidavit with a federal magistrate in support of their search warrant application. They filed the warrant application in the federal district that had the closest connection to the search to be executed. The information gathered by the warrant was limited: primarily the IP addresses of those that accessed Playpen and additional information that would aid in identifying what computer accessed the site and what individual used that computer.

---

argument. The government also argues that Defendant does not have standing to challenge the warrant because the alleged defect in the warrant, that it exceeded the magistrate’s jurisdiction, does not apply to him because his computer was in the Eastern District. Gov’t’s Resp. to Second Mot. at 8–9. This seems to be a novel interpretation of standing law in Fourth Amendment cases. The standing inquiry in Fourth Amendment cases asks if the individual seeking suppression had a reasonable expectation of privacy in the thing searched. See Rakas v. Illinois, 439 U.S. 128, 133–34 (1978). Defendant’s computer was searched, and he has a reasonable expectation of privacy in his computer.

Defendant seeks suppression because of an alleged violation of a Federal Rule of Criminal Procedure, a rule that will likely be changed to allow explicitly this type of search. The pending amendment is evidence that the drafters of the Federal Rules do not believe that there is anything unreasonable about a magistrate issuing this type of warrant; the Rules had simply failed to keep up with technological changes. That is, there is nothing unreasonable about the scope of the warrant itself. The FBI should be applauded for its actions in this case.

In short, the officers in charge of this investigation are not at all culpable. Additionally, as discussed above, there is no evidence that any failure by the FBI to understand the intricacies of the jurisdiction of federal magistrates was deliberate. Even if the NIT Warrant was void because not authorized by the Federal Magistrates Act, suppression is not warranted in this case.

In summary, the NIT Warrant did not violate Rule 41(b) and even if it did suppression is not warranted. Accordingly, the Court **DENIES** Defendant's Second Motion to Suppress. ECF No. 18.

### III. MOTION TO COMPEL

Defendant has belatedly filed a Motion to Compel last night at 11:49 pm. ECF No. 30. With this Motion, Defendant seeks a copy of the source code of the NIT used to search his computer. Id. Defendant alleges that the source code may show that the NIT did not comply with the conditions of the NIT Warrant and is thus critical to his First and Second Motions to Suppress.<sup>9</sup> Id. at 1–2. However, Defendant does not make this argument in either Motion to Suppress. Accordingly the Court decides the Motions to Suppress now and will consider the Motion to Compel when it is ripe.

### IV. CONCLUSION

For reasons set forth above, the Court **DENIES** Defendant's First Motion to Suppress,


---

<sup>9</sup> He also claims that the code is necessary for his trial preparation. ECF No. 30 at 2–3.

ECF No. 15, and **DENIES** Defendant's Second Motion to Suppress, ECF No. 18.

The Clerk is **DIRECTED** to forward a copy of this Order to all Counsel of Record.

**IT IS SO ORDERED.**

  
UNITED STATES DISTRICT JUDGE

Norfolk, VA  
June 3 2016

**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF WISCONSIN**

---

**UNITED STATES OF AMERICA,**

Plaintiff,

v.

**Case No. 15-CR-163**

**PHILLIP A. EPICH,**

Defendant.

---

**RECOMMENDATION ON DEFENDANT'S MOTION TO SUPPRESS**

---

On August 11, 2015, a grand jury sitting in the Eastern District of Wisconsin returned a two-count indictment against the defendant, Phillip A. Epich.

(Indictment, ECF No. 18.) Count One charges Mr. Epich with knowingly receiving child pornography, in violation of 18 U.S.C. § 2252A(a)(2), and Count Two charges Mr. Epich with knowingly possessing matter that contained images of child pornography, in violation 18 U.S.C. § 2252A(a)(5)(B). On August 19, 2015, Mr. Epich pled not guilty to both counts charged in the Indictment. (Minute entry for arraignment and plea hearing, ECF No. 24.) The matter is assigned to United States District Judge Rudolph T. Randa for trial and to this Court for pretrial motions. Trial in this matter is adjourned.

Currently pending before this Court is Mr. Epich's motion to suppress, which he filed on September 24, 2015. For the reasons that follow, the Court will recommend that Mr. Epich's motion to suppress be denied.



## I. Investigative Background

In September 2014, agents from the Federal Bureau of Investigation began investigating a website that appeared to be dedicated to the advertisement and distribution of child pornography. The website operated on the anonymous Tor network, which allowed users to mask their Internet Protocol addresses while accessing the website. In February 2015, the FBI apprehended the website's administrator and assumed administrative control of the site. The FBI allowed the site to continue to operate from a computer server that was located at a government facility in Newington, Virginia.

On February 20, 2015, a United States Magistrate Judge in the Eastern District of Virginia issued a warrant authorizing the government to deploy a network investigative technique (NIT) on the computer server running the seized website. (NIT Warrant and Application, ECF No. 41-1.) Essentially, the NIT allowed the government to obtain the true IP address of computers that logged onto the website. The government deployed the NIT from February 20, 2015, until March 4, 2015.

During the investigation, law enforcement agents identified "Redrobin16" as a user of the website. Agents obtained Redrobin16's IP address using the NIT, and subsequent investigation linked this IP address to Mr. Epich at his home in West Allis, Wisconsin. On July 16, 2015, United States Magistrate Judge William E. Duffin issued a warrant authorizing the search of Mr. Epich's residence. (Residence Warrant and Application, ECF No. 41-2.) Agents executed the warrant the following

day and recovered, among other things, a desktop computer that contained evidence of searching for and viewing child pornography. Mr. Epich was then arrested pursuant to a criminal complaint that charged him with receiving child pornography.

Agents subsequently seized a thumb drive that was kept in Mr. Epich's home but not found during the initial search. On August 6, 2015, United States Magistrate Judge Nancy Joseph issued a warrant authorizing the search of the thumb drive. (Thumb Drive Warrant and Application, ECF No. 41-3.) The thumb drive contained additional child pornography.

## **II. Discussion**

Mr. Epich seeks an order suppressing all evidence and derivative evidence obtained as a result of the searches of his home and property. (Motion to Suppress, ECF No. 34.) As grounds for his motion, Mr. Epich argues that the warrants to search his residence and thumb drive are invalid because they relied extensively on the "deeply flawed" NIT Warrant. (*Id.* at 1.) More precisely, he maintains that the government would not have been able to secure the Residence Warrant or the Thumb Drive Warrant without information—namely, his IP address—derived from the NIT Warrant. He further asserts that an evidentiary hearing is not necessary because his argument is limited to the four corners of the search warrant affidavits. (*Id.* at 1.) Thus, the Court will begin by summarizing the contents of those documents.

## A. Search warrants and supporting documents

On February 20, 2015, an FBI Special Agent applied for a warrant to use an NIT to investigate the users and administrators of a website that was believed to be dedicated to child pornography. In support of the warrant application, the agent submitted a thirty-three-page affidavit that set forth his basis for probable cause to believe that deploying the NIT would uncover evidence and instrumentalities of certain child exploitation crimes. (Affidavit in support of application for NIT Warrant [hereinafter NIT Warrant Affidavit], ECF No. 41-1 at 6-38.)

After describing background information concerning federal investigations related to child pornography and the sexual exploitation of children, (*id.* ¶¶ 1-5), the affidavit discusses the anonymous nature of the target website. The website operated on the anonymous Tor network, which users could access only after downloading specific Tor software. (*Id.* ¶ 7.) Use of “[t]he Tor software protect[ed] users’ privacy online by bouncing their communications around a distributed network of relay computers run by volunteers all around the world, thereby masking the user’s actual IP address.” (*Id.* ¶ 8.) Thus, the Tor network neutralized traditional methods utilized to identify users who visited particular websites. The Tor network also allowed users to host entire websites as “hidden services,” which prevented law enforcement agents and other users from determining the location of the host computer. (*Id.* ¶ 9.)

The affidavit then discusses how users could find and access the website. Because the website was set up as a hidden service, it did not reside on the

traditional Internet. (*Id.* ¶ 10.) Rather, a user could access the site only through the Tor network and only if the user knew the site’s exact web address. A user could learn the web address from other users of the site or from other Internet postings describing the site’s content and location. Given the “numerous affirmative steps” required to access the website, the affidavit states that it would be “extremely unlikely that any user could simply stumble upon [the site] without understanding its purpose and content.” (*Id.*) Further, the main page of the site contained “images of prepubescent females partially clothed and whose legs are spread.” (*Id.*) The affidavit thus concludes that any user who successfully accessed the website had knowingly done so with intent to view child pornography. (*Id.*)

Next, the affidavit describes the nature and content of the website. The site “appeared to be a message board website whose primary purpose [was] the advertisement and distribution of child pornography.” (*Id.* ¶ 11.) The first post was made in August 2014 and, at the time the affidavit was submitted, the website contained 95,148 posts, 9,333 total topics, and 158,094 members. The main page of the site contained “two images depicting partially clothed prepubescent females with their legs spread apart.” (*Id.* ¶ 12.) Text underneath the images read, “No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out.” (*Id.*) The affiant explained that, based on his training and experience, “no cross-board reports” referred to “a prohibition against material that is posted on other websites from being ‘re-posted’ to [the website],” and “.7z” referred to “a preferred method of compressing large files or sets of files for distribution.” (*Id.*)

Before logging onto the website, users had to register an account by accepting the site's registration terms and entering a username, password, and email address. (*Id.* ¶¶ 12-14.) The registration terms advised users to provide a fake email address and emphasized the anonymous nature of the site. (*Id.* ¶ 13.) The entire text of the registration terms was included in the affidavit. (*See id.*)

Upon registering and logging on, users could observe all the of sections, forums, and sub-forums contained on the website, along with the corresponding number of topics and posts in each category. (*Id.* ¶¶ 14-19.) Many of the sections were subdivided by age (e.g., "Jailbait" or "Pre-teen"), gender (boys or girls), and/or level of explicit conduct (hardcore or softcore). Several of the forums "contained general information in regards to the site, instructions and rules for how to post, and welcome messages between users." (*Id.* ¶ 17.) The remaining forums contained "numerous images that appeared to depict child pornography . . . and child erotica," and the affidavit describes, in graphic detail, several examples of images depicting prepubescent females being sexually abused by adult males. (*Id.* ¶ 18.) The website also contained a private messaging feature, which the affiant believed was used "to communicate regarding the dissemination of child pornography," as well as other features that were used to facilitate the advertisement, distribution, and sharing of child pornography. (*Id.* ¶¶ 20-25.)

After describing the identification and seizure of the website's administrator and host computer server, (*id.* ¶¶ 28-30), the affidavit details the NIT and how it would be deployed on the site. Given the anonymity provided by the Tor network,

traditional investigative procedures had failed or were unlikely to uncover the identities of the site's administrators and users. (*Id.* ¶ 31.) According to the affiant, however, the NIT had "a reasonable likelihood of securing the evidence necessary to prove beyond a reasonable doubt the actual location of those users and administrators of [the site]" who were violating federal laws concerning child pornography and the sexual exploitation of children. (*Id.*)

The NIT would be deployed each time a user logged onto the website while it was running on a computer server located at a government facility in the Eastern District of Virginia. (*Id.* ¶ 36.) The NIT involved additional computer instructions that would be downloaded to a user's computer along with the site's normal content. (*Id.* ¶ 33.) After downloading the additional instructions, the user's computer would transmit certain information to a government-controlled computer that was located in the Eastern District of Virginia, including: (1) the computer's actual IP address; (2) a unique identifier to distinguish the data from that of other computers; (3) the computer's operating system; (4) information about whether the NIT had already been delivered to the computer; (5) the computer's "Host Name"; (6) the computer's active operating system username; and (7) the computer's "Media Access Control" address. (*Id.* ¶¶ 33-34, 36.)

The affidavit describes how each category of information "may constitute evidence of the crimes under investigation, including information that may help to identify the . . . computer and its user." (*Id.* ¶ 35.) As just one example, the computer's actual IP address could be associated with an Internet Service Provider

and a particular ISP customer. The affidavit requested authorization to use the NIT for thirty days. (*Id.* ¶ 36.)

A United States Magistrate Judge in the Eastern District of Virginia signed the NIT Warrant on February 20, 2015. (NIT Warrant, ECF No. 41-1 at 3-5.) Agents executed the warrant that same day and continued to collect data from computers that accessed the website until March 4, 2015. (NIT Warrant Return, ECF No. 41-1 at 39-40.)

On July 16, 2015, an FBI Special Agent applied for a warrant to search a residence located in West Allis, Wisconsin. In support of the warrant application, the agent submitted a thirty-one-page affidavit that set forth his basis for probable cause to believe that the residence contained evidence relating to federal violations concerning child pornography. (Affidavit in support of application for Residence Warrant, ECF No. 41-2 at 10-40.)

After discussing the affiant's training and experience, the relevant statutes, and definitions of terms used therein, (*id.* ¶¶ 1-29), the affidavit describes the investigative background and the specific facts establishing probable cause. The affidavit indicates that Mr. Epich "[had] been linked to an online community of individuals who regularly send and receive child pornography via a website that operated on an anonymous online network." (*Id.* ¶ 30.) Reciting much of the information contained in the NIT Warrant Affidavit, the affidavit then describes the nature of the Tor network, the content of the website, and the government's use of the NIT. (*Id.* ¶¶ 31-48.)

Next, the affidavit explains how law enforcement agents identified Mr. Epich as a suspected user of the website. An individual with the username “Redrobin16” registered an account on the website on February 19, 2015, and accessed the site several times between February 19 and February 24, 2015. (*Id.* ¶¶ 49-54.) This user accessed several posts that contained links to and sample photos of child pornography. Agents learned the user’s IP address via the NIT, determined the service provider of the IP address, and linked the IP address to Mr. Epich at his residence in West Allis. (*Id.* ¶¶ 50-60.)

Judge Duffin signed the Residence Warrant on July 16, 2015, (Residence Warrant, ECF No. 41-2 at 1-8), and law enforcement agents executed it the following day, (Affidavit in support of application for Thumb Drive Warrant [hereinafter Thumb Drive Warrant Affidavit], ECF No. 41-3 at 6-13). During the search of Mr. Epich’s residence, agents recovered a desktop computer that contained evidence of searching for and viewing child pornography. (Thumb Drive Warrant Affidavit ¶ 5.) Mr. Epich was then arrested and charged in federal court with receiving child pornography. (*Id.* ¶ 6.) Subsequent investigation led agents to seize a thumb drive that Mr. Epich kept in his residence but which was not found during the initial search. (*Id.* ¶¶ 7-9.)

On August 6, 2015, an FBI Special Agent applied for a warrant to search the thumb drive. In support of the warrant application, the agent submitted an eight-page affidavit that set forth his basis for probable cause to believe that the thumb drive contained evidence relating to federal violations concerning child



pornography. The affidavit indicates that agents interviewed Mr. Epich and that he admitted to using his desktop computer to view child pornography. (*Id.* ¶ 6.) To establish probable cause, the affiant also attached a copy of the Residence Warrant and its supporting application and affidavit. (*See* ECF No. 41-3 at 14-53.)

Judge Joseph signed the Thumb Drive Warrant on August 6, 2015. (Thumb Drive Warrant, ECF No. 41-3 at 1-4.) Forensic analysis revealed that the thumb drive contained child pornography.

## **B. Analysis**

According to Mr. Epich, the NIT Warrant “was unique in scope and breadth.” (Mot. at 2.) More precisely, he argues that the warrant is deeply flawed because it “failed to establish probable cause, failed to meet the Fourth Amendment’s particularity requirements, failed to show that the searches would recover evidence of a crime, and violated the Federal Rules of Criminal Procedure.” (*Id.*) The Court will address each argument in turn.

### *1. The warrant’s compliance with the Fourth Amendment*

Mr. Epich first argues that the NIT Warrant failed to comport with the requirements of the Fourth Amendment. (*Id.* at 10-22.) Specifically, he maintains that the affidavit submitted in support of the NIT Warrant

failed to establish probable cause because it applied to any person who logged onto the website even though: (1) the website did not warn potential users that it contained illegal materials; (2) users can visit and use the website without looking at any illegal material; [and] (3) the warrant could have, but failed, to differentiate between different users.

(*Id.* at 10-19.) Thus, according to Mr. Epich, the NIT Warrant Affidavit failed to establish probable cause to believe that *every person* who logged onto the website committed a crime. (*Id.* at 19; Reply in Support of Motion to Suppress, ECF No. 47 at 2; Response to Government’s Sur-reply, ECF No. 52 at 1.) He further maintains that the affidavit failed to meet the Fourth Amendment’s particularity requirement because it did not explain how the government would ensure that “innocent” devices or individuals were not subject to search. (Mot. at 19-21.) Mr. Epich also contends that the affidavit failed to establish that the search would uncover evidence of a crime because the search applied to all users of the website without regard to whether they violated any law. (*Id.* at 21-22.)

The Fourth Amendment provides that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. “When an affidavit is the only evidence presented to a judge in support of a search warrant, the validity of the warrant rests solely on the strength of the affidavit.” *United States v. Peck*, 317 F.3d 754, 755 (7th Cir. 2003).

“A search warrant affidavit establishes probable cause when it ‘sets forth facts sufficient to induce a reasonable prudent person to believe that a search thereof will uncover evidence of a crime.’” *United States v. Jones*, 208 F.3d 603, 608 (7th Cir. 2000) (quoting *United States v. McNeese*, 901 F.2d 585, 592 (7th Cir. 1990)). In deciding whether an affidavit establishes probable cause, “courts must use the flexible totality-of-the-circumstances standard set forth in *Illinois v. Gates*,

462 U.S. 213, 238, 103 S. Ct. 2317, 2332, 76 L. Ed. 2d 527 (1983).” *McNeese*, 901 F.2d at 592. Applying the totality-of-the-circumstances standard, “[t]he task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place.” *Gates*, 462 U.S. at 238.

“[P]robable cause is a fluid concept -- turning on the assessment of probabilities in particular factual contexts.” *Id.* at 232. Thus, “[i]n dealing with probable cause, . . . as the very name implies, we deal with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act.” *Brinegar v. United States*, 338 U.S. 160, 175 (1949). “Probable cause denotes more than mere suspicion, but does not require certainty.” *United States v. Anton*, 633 F.2d 1252, 1254 (7th Cir. 1980).

The court’s duty in reviewing a search warrant and its supporting materials is limited to ensuring “that the magistrate had a ‘substantial basis for . . . [concluding]’ that probable cause existed.” *Gates*, 462 U.S. at 238-39 (quoting *Jones v. United States*, 362 U.S. 257, 271 (1960)). In other words,

a magistrate’s determination of probable cause is to be “given considerable weight and should be overruled only when the supporting affidavit, read as a whole in a realistic and common sense manner, does not allege specific facts and circumstances from which the magistrate could reasonably conclude that the items sought to be seized are associated with the crime and located in the place indicated.”

*United States v. Pritchard*, 745 F.2d 1112, 1120 (7th Cir. 1984) (quoting *United States v. Rambis*, 686 F.2d 620, 622 (7th Cir. 1982)). Even “doubtful cases should be resolved in favor of upholding the warrant.” *Rambis*, 686 F.2d at 622.

Here, Mr. Epich argues that the NIT Warrant Affidavit failed to establish probable cause to believe that every person who logged onto the website committed a crime because users could access the site without knowing its illegal nature and without violating the law. (Mot. at 19; Reply at 2; Resp. to Sur-reply at 1.) That is, according to Mr. Epich, logging onto a website that contains child pornography—in addition to other, legal material—is insufficient to establish probable cause to search every user of that site. (Mot. at 16-19 (citing *United States v. Coreas*, 419 F.3d 151 (2d Cir. 2005)).)

Upon reviewing the NIT Warrant and its supporting materials in light of the parties’ arguments and the relevant case law, the Court finds that Mr. Epich’s argument rests on a crabbed reading of the search warrant affidavit and suggests a heightened standard of probable cause not mandated by the Fourth Amendment. Accordingly, for the reasons described below, the Court is persuaded that the issuing magistrate judge had a substantial basis for concluding that, under the totality of the circumstances, there was a fair probability that evidence relating to federal violations concerning child pornography would be found by using the NIT on the target website.

A commonsense reading of the affidavit demonstrates that it is highly

unlikely that the NIT Warrant subjected to search users who stumbled upon the website by pure happenstance because users had to engage in numerous affirmative steps just to gain access to the site's content. The affidavit explained that the website operated on the anonymous Tor network, which users could access only after downloading specific Tor software. (NIT Warrant Affidavit ¶¶ 7-9.) It further explained that the website was not located on the traditional Internet and, thus, users had to know the exact web address to access the site. (*Id.* ¶ 10.) This Tor-based web address was simply “a series of algorithm-generated characters . . . followed by . . . ‘.onion.’” (*Id.* ¶ 9.) Thus, the web address was not something that could be easily remembered. The affidavit suggested that users could obtain the address via word of mouth or by clicking a link on a Tor “hidden service” page. (*Id.* ¶ 10.) By describing the nature of the website and the steps required to find it, the affidavit supported the reasonable inference that users likely discovered the web address via other forums dedicated to child pornography.

Moreover, although a user could accomplish the above steps with relative ease, other information contained in the affidavit bolstered the conclusion that it would be extremely unlikely that any user would access the site without understanding its purpose and content. That is, even assuming that an individual could inadvertently or innocently find the site, such users were not subject to the NIT Warrant unless he/she engaged in other activities that revealed the site's illegal nature.

After downloading the Tor software and obtaining the website's exact web

address, users arrived at the main page of the site. Straddling the site's name were "two images depicting partially clothed prepubescent females with their legs spread apart." (*Id.* ¶ 12.) While the images alone implied that the site contained illicit child pornography, this suggestion was reinforced by the text located immediately underneath the images, which read, "No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out." (*Id.*) The affiant explained that, based on his training and experience, "no cross-board reports" referred to "a prohibition against material that is posted on other websites from being 're-posted' to [the website]," and ".7z" referred to "a preferred method of compressing large files or sets of files for distribution." (*Id.*) These technical terms thus implied that the site contained images or videos and was not simply a discussion forum or chatroom. Consequently, the juxtaposition of the suggestive images and the text referencing terms associated with sharing images and/or videos created a strong inference that the site contained child pornography.

To gain access to the site's content, users also had to register an account by accepting the site's registration terms and entering a username, password, and email address. (*Id.* ¶¶ 12-14.) The registration page further supported the inference that the site contained illicit material by advising users to provide a fake email address and by emphasizing the anonymous nature of the site. Upon registering and logging on, users gained access to all of the sections, forums, and sub-forums on the website, many of which contained images and/or videos that depicted child pornography. (*See id.* ¶¶ 14-27.) Thus, once logged on, the illegal nature of the site

was readily apparent.

To summarize, the NIT Warrant Affidavit established the following facts regarding the target website and its registered users: (1) the website operated only on an anonymous network that required users to download specific software before even finding the site; (2) finding the site required multiple, intentional steps; (3) users were unlikely to find the site without knowing its purpose and content; (4) the main page of the site depicted images that suggested the site contained child pornography and text that implied the site contained illicit images and/or videos; (5) users needed to register an account before they could access the site's content and were encouraged to use a fake email address when registering; and (6) images and videos containing child pornography were available to all users who registered an account. Based on the totality of the circumstances, these facts created a reasonable inference that registered users who accessed the website knew that it contained child pornography and accessed the site with the intent to view this illicit material. Accordingly, the issuing magistrate judge had a substantial basis for concluding that probable cause existed to issue the NIT Warrant.

That the website also contained legal material, thereby making it possible that users could visit the site without violating the law, does not alter the analysis. While courts should consider "possible innocent alternatives" in the totality-of-the-circumstances analysis, it is well-established that "the mere existence of innocent explanations does not necessarily negate probable cause." *United States v. Funches*, 327 F.3d 582, 587 (7th Cir. 2003). Indeed, "probable cause

is far short of certainty—it ‘requires only a probability or substantial chance of criminal activity, not an actual showing of such activity.’” *United States v. Seiver*, 692 F.3d 774, 777 (7th Cir. 2012) (quoting *Gates*, 462 U.S. at 243 n.13). As described above, the totality-of-the-circumstances here established a substantial chance that registered users who accessed the website did so with the intent to view child pornography.

Similarly, the affidavit’s failure to differentiate users based on the frequency of log-ins, the duration of log-ins, or the material being accessed does not negate the probable cause finding. As other courts have accurately recognized, the probable cause analysis does not turn on what additional investigation the government *could have done*. See, e.g., *United States v. Shields*, 458 F.3d 269, 280 (3d Cir. 2006) (upholding validity of warrant authorizing search of defendant’s home even though FBI “could have” but did not “determine[] with certainty whether he actually downloaded illegal images”); *United States v. Gourde*, 440 F.3d 1065, 1072-73 & n.5 (9th Cir. 2006) (en banc) (same). The issuing judge had a substantial basis for finding probable cause even without the benefit of this additional information.

Furthermore, in contrast to Mr. Epich’s suggestion, the Second Circuit’s decision in *Coreas* does not demonstrate that probable cause was lacking in this case. In *Coreas*, a Second Circuit panel generally held that logging onto a website that contains child pornography—in addition to other, legal material—and agreeing to join its e-group does not establish probable cause to search that person’s home. *Coreas*, 419 F.3d at 156-59. A number of courts have reached the opposite



conclusion. *See, e.g., Shields*, 458 F.3d at 278-80; *Gourde*, 440 F.3d at 1069-73; *United States v. Froman*, 355 F.3d 882, 890-91 (5th Cir. 2004); *United States v. Hutto*, 84 F. App'x 6, 8 (10th Cir. 2003); *United States v. Bailey*, 272 F. Supp. 2d 822, 824-25 (D. Neb. 2003). Indeed, the *Coreas* court ultimately affirmed the defendant's conviction, finding that it was compelled by an earlier panel's decision that addressed the same issue and reached the opposite conclusion. *Coreas*, 419 F.3d at 157-59; *see United States v. Martin*, 426 F.3d 68, 74-77 (2d Cir. 2005).

Perhaps more importantly, the facts in *Coreas* are materially distinguishable from the facts at issue here. First, the court in *Coreas* implied that probable cause was lacking because there was no evidence that members knew the alleged "primary purpose" of the e-group or actually intended to take advantage of the site's illicit features. *Coreas*, 419 F.3d at 158. The court further emphasized that the search warrant affidavit did not allege that the defendant downloaded any child pornography. *Id.* at 156-57. Thus, probable cause was based solely on "clicking a button." *Id.* In this case, however, the information in the NIT Warrant Affidavit established a reasonable inference that registered users of the website knew its purpose and accessed the site with the intent to view child pornography. The users here also were subject to search only after downloading specific software, locating the website, registering an account, and logging onto the site during the two-week window the government deployed the NIT. Thus, probable cause was based on more significant conduct than simply clicking a button to join an online group.

Second, the warrant at issue in *Coreas* authorized the government "to enter

[the defendant's] private dwelling and rummage through various of his personal effects." *Coreas*, 419 F.3d at 156 (collecting cases). The NIT Warrant, in contrast, merely authorized use of the NIT to obtain information that would assist the government in identifying the website's users, namely their actual IP address. The NIT search was thus minimally invasive compared to the search authorized in *Coreas*. Of course, the information gathered from the NIT search led the government to seek warrants to search Mr. Epich's residence and a thumb drive found therein. However, the Residence Warrant and the Thumb Drive Warrant were issued only after the government conducted additional investigation that confirmed Mr. Epich had accessed from the website several posts that contained links to and sample photos of child pornography.

Mr. Epich's remaining Fourth Amendment arguments are unavailing and, therefore, require only a brief analysis. The Court finds that the NIT Warrant satisfied the Fourth Amendment's particularity requirement as it specifically described the place to be searched and the things to be seized. The search warrant affidavit outlined who would be subject to the NIT, what information the NIT would obtain from users' computers, when the NIT would be deployed; where the NIT would be deployed, why the NIT was necessary, and how the NIT would be deployed. (NIT Warrant Affidavit ¶¶ 31-37.) The affidavit also included Attachments A and B, which described, respectively, the "Place to be Searched" and the "Information to be Seized." (*See id.* at 32-33.) The affidavit further indicated that the NIT would reveal only the specific identifying information listed in

Attachment B. (*See id.* ¶ 34.) Thus, Mr. Epich’s contention that the NIT could have searched or infected innocent computers or devices, (Mot. at 20), is purely speculative and without merit.

Likewise, the information contained in the affidavit established a fair probability that deployment of the NIT would uncover evidence of a crime. In essence, the NIT would pierce the veil afforded by the anonymous Tor network and provide the government the information—i.e., the actual IP address—needed to ascertain the location and identity of the website’s users who accessed the site with the intent to view child pornography. (NIT Warrant Affidavit ¶¶ 31-37.) Put simply, such information constitutes evidence of a crime within the meaning of the Fourth Amendment.

In sum, for all the foregoing reasons, the Court finds that the NIT Warrant comported with the requirements of the Fourth Amendment.

*2. The warrant’s compliance with Federal Rule Criminal Procedure 41(b)*

Mr. Epich also argues that the NIT Warrant “plainly violated Rule 41 of the Federal Rules of Criminal Procedure” and that suppression is an appropriate remedy here because the violation was “prejudicial and blatant.” (*See* Mot. at 22-24; Reply at 17-22; Resp. to Sur-reply at 3-5.)

“Rule 41(b) sets out five alternative territorial limits on a magistrate judge’s authority to issue a warrant.” *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 756 (S.D. Tex. 2013). Specifically, Rule 41(b) authorizes magistrate judges to issue warrants to (1) search for and seize a

person or property located within the judge's district; (2) search for and seize a person or property located outside the judge's district "if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed"; (3) search for and seize a person or property located outside the judge's district if the investigation relates to terrorism; (4) "install within the district a tracking device . . . to track the movement of a person or property located within the district, outside the district, or both; or (5) search for and seize a person or property located outside the judge's district but within a United States territory, possession, commonwealth, or premises used by a United States diplomatic or consular mission. *See* Fed. R. Crim. P. 41(b).

The government argues that the NIT Warrant comported with the territorial limits set forth in Rule 41(b). (*See* Government's Response to Defendant's Motion to Suppress, ECF No. 41 at 32-35; Government's Sur-reply in Opposition to Defendant's Motion to Suppress, ECF No. 49 at 4-6.) According to the government, the NIT was essentially a set of computer instructions that the government deployed on the target website while it was running on a computer server located in the Eastern District of Virginia. When a user logged onto the website while the NIT was in effect, the user's computer downloaded the additional instructions from the server and then sent the requested information back to a server located in the Eastern District of Virginia. The government thus maintains that the NIT Warrant satisfied Rule 41(b)(1) or (b)(2) because the NIT was property located within the

district of the issuing judge and because users “reached into” the Eastern District of Virginia to access the seized website. The government also likens the NIT to a “tracking device” authorized under Rule 41(b)(4). Alternatively, the government argues that suppression is generally not an apt remedy for a Rule 41 violation and that suppression would be especially inappropriate in this case because users relied on an anonymous network to mask their identities.

Mr. Epich argues that the NIT Warrant does not fall within any of the five provisions listed in Rule 41(b). According to Mr. Epich, the NIT Warrant authorized the government to search his computer—i.e., property that was never located within the Eastern District of Virginia, let alone at the time the warrant was issued. (Reply at 17-20.) He also maintains that the identifying information sought by the warrant was not sent into the Eastern District of Virginia until users logged onto the website *after* the warrant was executed. Mr. Epich further contends that the NIT cannot be considered a tracking device because it did not track the movement of users’ computers and, in any case, the NIT was not installed within the Eastern District of Virginia.

Although Mr. Epich raises an interesting and compelling issue,<sup>1</sup> the Court

---

<sup>1</sup> Indeed, the Supreme Court is currently reviewing a proposed amendment to Rule 41(b) that would allow magistrate judges “to issue a warrant to use remote access to search electronic storage media” located inside or outside the judge’s district if “the district where the media or information is located has been concealed through technological means.” *See* Advisory Committee on Criminal Rules, September 2015 Agenda, at 205, available at <http://www.uscourts.gov/rules-policies/records-and-archives-rules-committees/agenda-books>); *see also* United States Courts, Pending Rules Amendments, <http://www.uscourts.gov/rules-policies/pending-rules-amendments> (last visited Jan. 21, 2016).

need not determine whether the NIT Warrant strictly complied with the requirements of Rule 41(b) to resolve Mr. Epich's motion because suppression clearly would not be an appropriate remedy in this case. The Seventh Circuit has unequivocally held that "violations of federal rules do not justify the exclusion of evidence that has been seized on the basis of probable cause, and with advance judicial approval." *United States v. Cazares-Olivas*, 515 F.3d 726, 730 (7th Cir. 2008). The court has also explicitly rejected suppression as a remedy for a Rule 41 violation, holding that "[t]he remedy of allowing a defendant to go free based on a violation of Rule 41's requirements for obtaining a proper search warrant would be 'wildly out of proportion to the wrong.'" *United States v. Berkos*, 543 F.3d 392, 396 (7th Cir. 2008) (quoting *Cazares-Olivas*, 515 F.3d at 730). Moreover, the court has expressed doubt as to whether suppression would ever be an appropriate remedy for such a violation:

In light of *Leon*, it is difficult to anticipate any violation of Rule 41, short of a defect that also offends the Warrant Clause of the fourth amendment, that would call for suppression. Many remedies may be appropriate for deliberate violations of the rules, but freedom for the offender is not among them.

*United States v. Trost*, 152 F.3d 715, 721-22 (7th Cir. 1998) (quoting *United States v. Hornick*, 815 F.2d 1156, 1158 (7th Cir. 1987)).

Consequently, even assuming that the NIT Warrant violated Rule 41(b), the evidence at issue here should not be suppressed because it was obtained via a judicially authorized warrant supported by probable cause. Suppression would be an especially inappropriate remedy in this case given the circumstances facing the

government. Because of the anonymizing software, the government was unable to determine the location and identity of the website's users. The NIT, however, provided the government the means to unmask these users, who were suspected of committing federal violations concerning child pornography. Likewise, the government sought the NIT Warrant in the judicial district where the seized website was located and where the NIT was to be implemented. Such conduct was reasonable under the circumstances.

Accordingly, because the NIT Warrant satisfied the requirements of the Fourth Amendment, and because suppression would be "wildly out of proportion" to any purported violation of Rule 41(b), the Court will recommend that the district judge deny Mr. Epich's motion to suppress.

**NOW, THEREFORE, IT IS HEREBY RECOMMENDED** that defendant Phillip A. Epich's motion to suppress, (ECF No. 34), be **DENIED**.

Your attention is directed to General L. R. 72(c) (E.D. Wis.), 28 U.S.C. § 636(b)(1)(B), and Federal Rules of Criminal Procedure 59(b) or 72(b), if applicable, whereby written objections to any recommendation herein, or part thereof, may be filed within fourteen days of the date of service of this recommendation. Objections are to be filed in accordance with the Eastern District of Wisconsin's electronic case filing procedures. Courtesy paper copies of any objections shall be sent directly to the chambers of the district judge assigned to the case. Failure to file a timely objection with the district court shall result in a waiver of a party's right to appeal. If no response or reply will be filed, please notify the Court in writing.

Dated at Milwaukee, Wisconsin, this 21st day of January, 2016.

**BY THE COURT:**

*s/ David E. Jones* \_\_\_\_\_  
DAVID E. JONES  
United States Magistrate Judge



UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF WISCONSIN

---

UNITED STATES OF AMERICA,

Case No. 15-CR-163-PP

Plaintiff,

v.

PHILLIP A. EPICH,

Defendant.

---

**DECISION AND ORDER ADOPTING MAGISTRATE JUDGE'S REPORT AND  
RECOMMENDATION (DKT. NO. 53) AND DENYING DEFENDANT'S MOTION  
TO SUPPRESS (DKT. NO. 34)**

---

On August 11, 2015, defendant Phillip A. Epich was indicted by a federal grand jury on charges that he knowingly received child pornography and that he knowingly possessed matter containing images of child pornography. Dkt. No. 1. On September 24, 2015, the defendant filed a motion to suppress evidence seized pursuant to a search warrant. Dkt. No. 34 (sealed). The defendant asserted that the search of the defendant's home had resulted from a warrant issued in Virginia, giving the FBI permission to use a "Network Investigative Technique" ("NIT") to determine the identities of registered users of an anonymous web site hosted through a network called "Tor." *Id.* at 7-8. The defendant argued that the Virginia warrant failed to establish probable cause, was not specific in describing how the NIT would find users of the web site and how it would make sure to find only users who were engaged in illegal activity,

did not demonstrate that the NIT was likely to reveal evidence of a crime, and was unlimited in geographic scope. Id. at 10-11.

The government responded to the motion to suppress on October 23, 2015, Dkt. No. 25, and Magistrate Judge David E. Jones issued a report and recommendation on January 21, 2016, Dkt. No. 53. Judge Jones found the defendant's arguments unpersuasive, and recommended that this court deny the defendant's motion to suppress. Id.

The court has reviewed Judge Jones' January 21, 2016 report and recommendation. Judge Jones first disagreed with the defendant's argument that the Virginia warrant was flawed because it did not present sufficient evidence to prove that every person who logged on to the particular web site at issue (which operated through the Tor network, a network which allowed users to mask their IP addresses while they were using any sites on the network). Id. at 13. Judge Jones pointed to the complicated machinations through which users had to go to access the web site (meaning that unintentional users were unlikely to stumble onto it), id. at 14; the fact that the web site's landing page contained images of "partially clothes prepubescent females with their legs spread apart," id. at 15; the existence of statements on the landing page that made it clear that users were not to re-post materials from other web sites, and provided information for compressing large files (such as video files) for distribution, id.; the fact that the site required people to register to use it, and advised registrants to use fake e-mail addresses and emphasized that the site was anonymous, id.; and the fact that once a user went through all of *those*

steps to become a registered user, the user had access to the entire site, which contained “images and/or videos that depicted child pornography,” id. at 14-15. The combination of these facts convinced Judge Jones that anyone who ended up as a registered user on the web site was aware that the site contained, among other things, pornographic images of children. Id. at 15.

Judge Jones also found that the fact that one could become a registered user to the web site, and then view only information that did not contain illegal material, did not affect the probable cause determination that the Virginia magistrate judge made in issuing the warrant. Id. at 16-17. As Judge Jones pointed out, the Seventh Circuit has held that “the mere existence of innocent explanations does not necessarily negate probable cause.” Id. at 16 (citing United States v. Funches, 327 F.3d 582, 587 (7th Cir. 2003)). He found that the fact that the affidavit did not seek to use the NIT to find only frequent users, or only long-term users, did not affect probable cause; the question was whether the information that was presented in the affidavit provided sufficient probable cause, and Judge Jones (and the Virginia magistrate judge) determined that it did. Id. at 17.

Judge Jones also distinguished, on a number of grounds, the Second Circuit case upon which the defendant had relied, United States v. Coreas, 419 F.3d 151 (2nd Cir. 2015). He first pointed out that the Coreas decision (which generally held that “logging on to a website that contains child pornography—in addition to other, legal material—and agreeing to join its e-group does not establish probable cause to search that person’s home”—stood in contract to

several other courts' decisions to the contrary. Id. at 17-18. He also identified two key differences between the Coreas fact pattern and the defendant's: there was no evidence that the e-group members in Coreas knew the primary purpose of the site they visited, or intended to use any "illicit features," id. at 18; and the warrant in Coreas authorized the fully-intrusive search of the defendant's home and belongings, as opposed to the less intrusive search of web site data authorized by the Virginia warrant in this case, id. at 18-19.

Judge Jones rejected the defendant's argument that the warrant did not comply with the Fourth Amendment particularity requirement, pointing out that it explained who was subject to the search, what information the NIT would obtain, the time period during which the NIT would be used, and how it would be used, as well as bearing attachments describing the place to be searched and the information to be seized. Id. at 19. He also concluded that the warrant contained sufficient information to indicate a probability that the NIT would uncover evidence of a crime, again referring back to the lengths to which the site had gone to make itself anonymous and un-discoverable, and the fact that no registered user could be unaware that the site contained child pornography. Id. at 20.

Finally, Judge Jones rejected the defendant's argument that, because the Virginia warrant was not limited in geographic scope—in other words, because the NIT could capture data about users who physically might be located all over the map—it violated Federal Rule of Criminal Procedure 41, which sets geographic limits on a magistrate judge's authority to issue a warrant. Id.

Judge Jones noted, as an aside, that the Supreme Court currently was reviewing a proposed amendment to Rule 41 that would address this very issue. Id. at 22 n.1. To the main point, however, Judge Jones found, as the Seventh Circuit has done, that “violations of federal rules do not justify the exclusion of evidence that has been seized on the basis of probable cause, and with advance judicial approval.” Id. at 23 (citing United States v. Cazares-Olivas, 515 F.3d 726, 730 (7th Cir. 2008)). Suppression of evidence is rarely, if ever, the remedy for a violation of Rule 41, even if such a violation has occurred. Id. (citing United States v. Berkos, 543 F.3d 392, 396 (7th Cir. 2008)).

The defendant has not objected to Judge Jones’ recommendation that this court deny the defendant’s motion to suppress. While this court is not bound to accept that recommendation, the court’s own review of the pleadings and Judge Jones’ decision convince this court that Judge Jones’ decision was the correct one. This court finds that there was probable cause for the Virginia warrant to issue, and thus that the resulting search of the defendant’s home, electronic devices and thumb drive did not violate the Fourth Amendment.

For these reasons, the court adopts Judge Jones’ report and recommendation in whole, and incorporates his conclusions and the reasoning supporting those conclusions into this order.

The court **ORDERS** that the defendant’s October 8, 2015 motion to suppress evidence is **DENIED**. (Dkt. No. 34) The court will schedule a

telephonic status conference to discuss setting a final pretrial and trial date.

Dated in Milwaukee, Wisconsin this 14th day of March, 2016.

**BY THE COURT:**

A handwritten signature in black ink, consisting of a large, stylized loop followed by a horizontal line extending to the right.

**HON. PAMELA PEPPER**  
**United States District Judge**

UNITED STATES DISTRICT COURT  
DISTRICT OF MASSACHUSETTS

<hr/>		)	
UNITED STATES OF AMERICA,		)	
		)	
		)	
		)	
	v.	)	CRIMINAL ACTION
		)	NO. 15-10271-WGY
ALEX LEVIN,		)	
		)	
	Defendant.	)	
<hr/>		)	

YOUNG, D.J.

May 5, 2016

**AMENDED MEMORANDUM & ORDER**

**I. INTRODUCTION**

Alex Levin is charged with possession of child pornography. Compl. 1, ECF No. 1. The government obtained evidence of Levin's alleged crime in three steps. First, it seized control of a website that distributed the illicit material at issue ("Website A"). Next, it obtained a series of search warrants that allowed the government to identify individual users who were accessing content on Website A. One of these warrants involved the deployment of a Network Investigative Technique (the "NIT Warrant"). Finally, the government searched<sup>1</sup> the computers of certain of these individuals, including Levin.

---

<sup>1</sup> The government has waived any argument that its investigative conduct here did not amount to a search by failing to raise this argument in its memorandum. The Court therefore assumes that Levin had a reasonable expectation of privacy as to

Levin has moved to suppress the evidence obtained as a result of the issuance of the NIT Warrant, arguing that the NIT Warrant is void for want of jurisdiction under the Federal Magistrates Act, 28 U.S.C. § 636(a), and additionally that it violated Federal Rule of Criminal Procedure 41(b). Def.'s Mot. Suppress Evidence ("Def.'s Mot.") 5-6, ECF No. 44. The government contends that the NIT Warrant was valid and that, in any event, suppression is not an appropriate remedy on these facts. Gov't's Resp. Def.'s Mot. Suppress ("Gov't's Resp.") 1, ECF No. 60.

## **II. FACTUAL BACKGROUND**

This case involves a far-reaching and highly publicized investigation conducted by the Federal Bureau of Investigation in early 2015 to police child pornography.<sup>2</sup> The investigation focused on Website A, which was accessible to users only through

---

the information obtained through the execution of the various warrants.

<sup>2</sup> For coverage of this investigation, see, for example, Ellen Nakashima, [This is How the Government is Catching People Who Use Child Porn Sites](https://www.washingtonpost.com/world/national-security/how-the-government-is-using-malware-to-ensnare-child-porn-users/2016/01/21/fb8ab5f8-bec0-11e5-83d4-42e3bceea902_story.html), Wash. Post, Jan 21, 2016, [https://www.washingtonpost.com/world/national-security/how-the-government-is-using-malware-to-ensnare-child-porn-users/2016/01/21/fb8ab5f8-bec0-11e5-83d4-42e3bceea902\\_story.html](https://www.washingtonpost.com/world/national-security/how-the-government-is-using-malware-to-ensnare-child-porn-users/2016/01/21/fb8ab5f8-bec0-11e5-83d4-42e3bceea902_story.html); Mary-Ann Russon, [FBI Crack Tor and Catch 1,500 Visitors to Biggest Child Pornography Website on the Dark Web](http://www.ibtimes.co.uk/fbi-crack-tor-catch-1500-visitors-biggest-child-pornography-website-on-the-dark-web), Int'l Bus. Times, Jan. 6, 2016, <http://www.ibtimes.co.uk/fbi-crack-tor-catch-1500-visitors-biggest-child-pornography-website-dark-web-1536417>.



the "Tor" network -- software designed to preserve users' anonymity by masking their IP addresses.<sup>3</sup> See Def.'s Mot., Ex. 3, Aff. Supp. Application Search Warrant ("Aff. Supp. NIT Warrant") 10-12, ECF No. 44-3.

As an initial step in their investigation, FBI agents seized control of Website A in February 2015. See id. at 21-23. Rather than immediately shutting it down, agents opted to run the site out of a government facility in the Eastern District of Virginia for two weeks in order to identify -- and ultimately, to prosecute -- users of Website A. See id. at 23. To do this

---

<sup>3</sup> "Tor," which stands for "The Onion Router," is "the main browser people use to access" the "Darknet" -- "a specific part of th[e] hidden Web where you can operate in total anonymity." Going Dark: The Internet Behind the Internet, Nat'l Pub. Radio, May 25, 2014, <http://www.npr.org/sections/alltechconsidered/2014/05/25/315821415/going-dark-the-internet-behind-the-internet>. Tor itself is lawful and has various legitimate uses. See id. Indeed, it was developed by the United States Navy, which continues to use it "as a means of communicating with spies and informants[.]" John Lanchester, When Bitcoin Grows Up, 28 London R. Books No. 8, <http://www.lrb.co.uk/v38/n08/john-lanchester/when-bitcoin-grows-up>. Tor has, however, produced difficulties for law enforcement officials, "especially those pursuing child pornography, Internet fraud and black markets," since it allows criminals to evade detection. Martin Kaste, When a Dark Web Volunteer Gets Raided by the Police, Nat'l Pub. Radio, April 4, 2016, <http://www.npr.org/sections/alltechconsidered/2016/04/04/472992023/when-a-dark-web-volunteer-gets-raided-by-the-police>; see also Lanchester, supra (describing Tor as "the single most effective web tool for terrorists, criminals and paedos" and noting that it "gives anonymity and geographical unlocatability to all its users"). At the same time, its legal users have raised concerns about the privacy implications of government "sting" operations on the Tor network. See Kaste, supra.

required the deployment of certain investigative tools. See id. at 23-24.

To that end, the government sought and obtained a series of warrants. First, on February 20, 2015, the government procured an order pursuant to Title III from a district judge in the Eastern District of Virginia permitting the government to intercept communications between Website A users. Def.'s Mot., Ex. 2 ("Title III Warrant"), ECF No. 44-2. Second, also on that date, the government obtained a warrant from a magistrate judge in the Eastern District of Virginia to implement a Network Investigative Technique ("NIT") that would allow the government covertly to transmit computer code to Website A users.<sup>4</sup> NIT Warrant, ECF No. 44-3. This computer code then generated a communication from those users' computers to the government-operated server containing various identifying information, including those users' IP addresses.<sup>5</sup> See Aff. Supp. NIT Warrant 24-26.

---

<sup>4</sup> For a discussion of the government's recent use of these types of warrants, see Brian L. Owsley, Beware of Government Agents Bearing Trojan Horses, 48 Akron L. Rev. 315 (2015).

<sup>5</sup> The affidavit the government submitted in support of its application for the NIT Warrant describes this process:

In the normal course of operation, websites send content to visitors. A user's computer downloads that content and uses it to display web pages on the user's computer. Under the NIT authorized by this warrant,

Through the use of the NIT, government agents determined that a Website A user called "Manakaralupa" had accessed several images of child pornography in early March 2015, and they traced the IP address of that user to Levin's home address in Norwood, Massachusetts. Def.'s Mot., Ex. 1 ("Residential Warrant"), Aff. Supp. Application for Search Warrant ("Aff. Supp. Residential

---

[Website A], which will be located . . . in the Eastern District of Virginia, would augment that content with additional computer instructions. When a user's computer successfully downloads those instructions from [Website A] . . . the instructions, which comprise the NIT, are designed to cause the user's 'activating' computer to transmit certain information to a computer controlled by or known to the government.

Aff. Supp. NIT Warrant 24. The particular information seized pursuant to the NIT Warrant included:

1. the 'activating' computer's actual IP address, and the date and time that the NIT determines what that IP address is;
2. a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish data from that of other 'activating' computers, that will be sent with and collected by the NIT;
3. the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);
4. information about whether the NIT has already been delivered to the 'activating' computer;
5. the 'activating' computer's Host Name;
6. the 'activating' computer's active operating system username; and
7. the 'activating' computer's media access control ('MAC') address[.]

NIT Warrant, Attach. B (Information to be Seized).

Warrant") 11-12, ECF No. 44-1. On August 11, 2015, law enforcement officials obtained a third and final warrant (the "Residential Warrant") from Magistrate Judge Bowler in this District to search Levin's home. See Residential Warrant. Agents executed the Residential Warrant on August 12, 2015, and in their search of Levin's computer, identified eight media files allegedly containing child pornography. See Compl., Ex. 2, Aff. Supp. Application Criminal Compl. ¶ 7, ECF No. 1-2.

Levin was subsequently indicted on one count of possession of child pornography, 18 U.S.C. § 2252A(a)(5)(B). Indictment, ECF No. 8. He has since moved to suppress all evidence seized pursuant to the NIT Warrant and the Residential Warrant.<sup>6</sup> Def.'s Mot. After holding a hearing on March 25, 2016, the Court took Levin's motion under advisement. See Elec. Clerk's Notes, ECF No. 62.

### **III. ANALYSIS**

In support of his motion to suppress, Levin contends that the NIT Warrant violated the territorial restrictions on the issuing magistrate judge's authority,<sup>7</sup> and further that the

---

<sup>6</sup> The government does not contest Levin's argument that absent the NIT Warrant, it would not have had probable cause to support its Residential Warrant application, see Def.'s Mot. 14. For the sake of simplicity, the Court uses the phrase "evidence seized pursuant to the NIT Warrant" to include evidence seized pursuant to the Residential Warrant because all of that evidence is derivative of the NIT Warrant.

evidence obtained pursuant to the NIT Warrant must be suppressed in light of law enforcement agents' deliberate disregard for the applicable rules and the prejudice Levin suffered as a consequence. See Def.'s Mot. 6-7. The government refutes each of these arguments, and additionally argues that the good-faith exception to the exclusionary rule renders suppression inappropriate. See Gov't's Resp. 1.

**A. Magistrate Judge's Authority Under the Federal Magistrates Act and Rule 41(b)**

Levin argues that the issuance of the NIT Warrant ran afoul of both Section 636(a) of the Federal Magistrates Act and Rule 41(b) of the Federal Rules of Criminal Procedure. See Def.'s Mot. 5-7, 12. The conduct underlying each of these alleged violations is identical: the magistrate judge's issuance of a warrant to search property located outside of her judicial

---

<sup>7</sup> A more precise characterization of Levin's challenge would be that the magistrate judge who issued the NIT Warrant had no authority to do so under the relevant statutory framework and federal rules -- not that the issuance of the warrant "violated" these provisions, by, for example, failing to comply with procedural requirements. In the Court's view, this distinction is meaningful, see infra Part III(B)(1), though it is one that neither the parties nor other courts evaluating similar challenges seem to appreciate, see, e.g., United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263 at \*5-\*7 (W.D. Wash. Jan. 28, 2016) (discussing whether the NIT Warrant "violates" Federal Rule of Criminal Procedure 41(b)). In the interest of consistency with the parties' briefings and prior caselaw, however, the Court continues the tradition of referring to actions by a magistrate judge that fall outside the scope of her authority as "violations" of the provisions that confer such authority.

district. See id. Moreover, because Section 636(a) expressly incorporates any authorities granted to magistrate judges by the Federal Rules of Criminal Procedure, see infra Part III(A)(1), the Court's analyses of whether the NIT Warrant was statutorily permissible and whether it was allowed under Rule 41(b) are necessarily intertwined.

### 1. Federal Magistrates Act

Section 636(a) of the Federal Magistrates Act establishes "jurisdictional limitations on the power of magistrate judges[.]" United States v. Krueger, 809 F.3d 1109, 1122 (10th Cir. 2015) (Gorsuch, J., concurring). It provides, in relevant part:

(a) Each United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law--

(1) all powers and duties conferred or imposed . . . by law or by the Rules of Criminal Procedure[.]

28 U.S.C. § 636(a). Levin argues that the magistrate judge's issuance of a warrant to search property outside of her judicial district violated the territorial restrictions provided in the first paragraph of Section 636(a). Def.'s Mot. 12. In other words, because the NIT Warrant approved a search of property outside the Eastern District of Virginia ("the district in which sessions are held by the court that appointed the magistrate"),

and neither of the other clauses in the first paragraph of Section 636(a) applies, Levin contends that the magistrate judge lacked jurisdiction to issue it. See id. The government, for its part, notes that Levin does not meaningfully distinguish between the requirements of the statute and of Rule 41(b), and advances the same arguments to support the magistrate judge's authority to issue the NIT Warrant under Section 636(a) and under Rule 41(b). Gov't's Resp. 21.

As discussed in more detail infra Part III(A)(2)(i), the Court is persuaded by Levin's argument that the NIT Warrant indeed purported to authorize a search of property located outside the district where the issuing magistrate judge sat. The magistrate judge had no jurisdiction to issue such a warrant under the first paragraph of Section 636(a). The Court also concludes that Section 636(a)(1) is inapposite because Rule 41(b) did not confer on the magistrate judge authority to issue the NIT Warrant Levin challenges here, see infra Part III(A)(2), and the government points to no other "law or . . . Rule[] of Criminal Procedure" on which the magistrate judge could have based its jurisdiction pursuant to Section 636(a)(1), see infra note 11. Consequently, the Court holds that the Federal Magistrates Act did not authorize the magistrate judge to issue the NIT Warrant here.

## 2. Rule 41(b)

Rule 41(b), titled "Authority to Issue a Warrant,"

provides as follows:

At the request of a federal law enforcement officer or an attorney for the government:

(1) a magistrate judge with authority in the district -- or if none is reasonably available, a judge of a state court of record in the district -- has authority to issue a warrant to search for and seize a person or property located within the district;

(2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;

(3) a magistrate judge -- in an investigation of domestic terrorism or international terrorism -- with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;

(4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and

(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:

(A) a United States territory, possession, or commonwealth;

(B) the premises -- no matter who owns them -- of a United States diplomatic or consular mission in a foreign state, including any appurtenant



building, part of a building, or land used for the mission's purposes; or

(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

Fed. R. Crim. P. 41(b).

The government argues for a liberal construction of Rule 41(b) that would authorize the type of search that occurred here pursuant to the NIT Warrant. See Gov't's Resp. 18-20.

Specifically, it argues that subsections (1), (2), and (4) of Rule 41(b) are each sufficient to support the magistrate judge's issuance of the NIT Warrant. Id. This Court is unpersuaded by the government's arguments. Because the NIT Warrant purported to authorize a search of property located outside the Eastern District of Virginia, and because none of the exceptions to the general territorial limitation of Rule 41(b)(1) applies, the Court holds that the magistrate judge lacked authority under Rule 41(b) to issue the NIT Warrant.

**i. Rule 41(b)(1)**

The government advances two distinct lines of argument as to why Rule 41(b)(1) authorizes the NIT Warrant. One is that all of the property that was searched pursuant to the NIT Warrant was actually located within the Eastern District of Virginia, where the magistrate judge sat: since Levin -- as a

user of Website A -- "retrieved the NIT from a server in the Eastern District of Virginia, and the NIT sent [Levin's] network information back to a server in that district," the government argues the search it conducted pursuant to the NIT Warrant properly can be understood as occurring within the Eastern District of Virginia. Gov't's Resp. 20. This is nothing but a strained, after-the-fact rationalization. In its explanation of the "Place to be Searched," the NIT Warrant made clear that the NIT would be used to "obtain[] information" from various "activating computers[.]"<sup>8</sup> NIT Warrant 32. As is clear from Levin's case -- his computer was located in Massachusetts -- at least some of the activating computers were located outside of the Eastern District of Virginia. That the Website A server is located in the Eastern District of Virginia is, for purposes of Rule 41(b)(1), immaterial, since it is not the server itself from which the relevant information was sought. See United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263 at \*6 (W.D. Wash. Jan. 28, 2016) (examining the permissibility of the

---

<sup>8</sup> That the cover page of the NIT Warrant application indicated that the property to be searched was located in the Eastern District of Virginia, see NIT Warrant 1, does not alter this conclusion. See Michaud, 2016 WL 337263 at \*4 (observing that to read this NIT Warrant as authorizing a search of property located exclusively within the Eastern District of Virginia, on the basis of its cover page, is "an overly narrow reading of the NIT Warrant that ignores the sum total of its content." ).

same NIT Warrant and concluding that Rule 41(b)(1) did not authorize the search "because the object of the search and seizure was Mr. Michaud's computer, not located in the Eastern District of Virginia").

The government's other argument is that where, as here, it is impossible to identify in advance the location of the property to be searched, Rule 41(b)(1) ought be interpreted to allow "a judge in the district with the strongest known connection to the search" to issue a warrant. See Gov't's Resp. 20. This argument fails, though, because it adds words to the Rule. See Lopez-Soto v. Hawayek, 175 F.3d 170, 173 (1st Cir. 1999) ("Courts have an obligation to refrain from embellishing statutes by inserting language that Congress opted to omit.").

**ii. Rule 41(b)(2)**

Rule 41(b)(2) confers on magistrate judges the authority "to issue a warrant of a person or property outside the district if the person or property is located within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed." Fed. R. Crim. P. 41(b)(2). The government argues that because the NIT (i.e., the computer code used to generate the identifying information from users' computers) was located in the Eastern District of Virginia at the time the warrant was issued, this subsection applies. Gov't's Resp. 19. As discussed above, however, the

actual property to be searched was not the NIT nor the server on which it was located, but rather the users' computers.

Therefore, Rule 41(b)(2) is inapposite.

**iii. Rule 41(b)(4)**

The Court is similarly unpersuaded by the government's argument regarding Rule 41(b)(4), which authorizes magistrate judges in a particular district "to issue a warrant to install within the district a tracking device," even where the person or property on whom the device is installed later moves outside the district, see Fed. R. Crim. P. 41(b)(4). The government likens the transmittal of the NIT to Website A users' computers to the installation of a tracking device in a container holding contraband, insofar as each permits the government to identify the location of illegal material that has moved outside the relevant jurisdiction. Gov't's Resp. 19-20. This analogy does not persuade the Court that the NIT properly may be considered a tracking device, regardless of where the "installation" occurred.<sup>9</sup>

---

<sup>9</sup> Indeed, as the court pointed out in Michaud, which involved the same NIT Warrant:

If the 'installation' occurred on the government-controlled computer, located in the Eastern District of Virginia, applying the tracking device exception breaks down, because [users of Website A] never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular district. If the installation occurred on [the

**B. Suppression**

Having concluded that neither the Federal Magistrates Act nor Rule 41(b) authorized the issuance of the NIT Warrant, the Court now turns to the question of whether suppression of the evidence obtained pursuant to the NIT Warrant is an appropriate remedy. Levin argues that this evidence ought be suppressed because the magistrate judge lacked jurisdiction to issue the NIT Warrant and because Levin was prejudiced by the Rule 41 violation. Def.'s Mot. 13-14. The government argues that even if the issuance of the NIT Warrant was not sanctioned by Rule 41 or Section 636(a), suppression is too extreme a remedy, as any violation of the relevant rule or statute was merely ministerial and there was no resulting prejudice to Levin. Gov't's Resp.

---

individual Website A user's] computer, applying the tracking device exception again fails, because [the user's] computer was never physically located within the Eastern District of Virginia.

2016 WL 337263 at \*6. In any case, the Court is persuaded by the Southern District of Texas's interpretation of "installation." See In re Warrant to Search a Target Computer at Premises Unknown, 958 F.Supp.2d 753, 758 (S.D. Tex. 2013) (rejecting government's application for a warrant remotely to extract identifying information from a computer in an unknown location, noting that "there is no showing that the installation of the 'tracking device' (i.e. the software) would take place within this district. To the contrary, the software would be installed on a computer whose location could be anywhere on the planet."). Under that approach, the "installation" of the NIT occurred not within the Eastern District of Virginia, where the server is located, but rather at the site of each user's computer. See id.

16. Further, the government contends that the good-faith exception to the exclusionary rule ought preclude suppression of the evidence seized. Id. at 21-23.

The Court concludes that the violation at issue here is distinct from the technical Rule 41 violations that have been deemed insufficient to warrant suppression in past cases, and, in any event, Levin was prejudiced by the violation. Moreover, the Court holds that the good-faith exception is inapplicable because the warrant at issue here was void ab initio.

#### **1. Nature of the Rule 41 Violation**

A violation of Rule 41 that is purely technical or ministerial gives rise to suppression only where the defendant demonstrates that he suffered prejudice as a result of the violation. See United States v. Bonner, 808 F.2d 864, 869 (1st Cir. 1986). The government apparently submits that all Rule 41 violations "are essentially ministerial," and accordingly that suppression is an inappropriate remedy absent a showing of prejudice. Gov't's Resp. 16 (citing United States v. Burgos-Montes, 786 F.3d 92, 109 (1st Cir. 2015)).

Rule 41, however, has both procedural and substantive provisions -- and the difference matters. Courts faced with violations of Rule 41's procedural requirements have generally found such violations to be merely ministerial or technical, and

as a result have determined suppression to be unwarranted.<sup>10</sup> By contrast, this case involves a violation of Rule 41(b), which is “a substantive provision[.]” United States v. Berkos, 543 F.3d 392, 398 (7th Cir. 2008); see also United States v. Krueger, 809 F.3d 1109, 1115 n.7 (10th Cir. 2015) (noting that Rule 41(b)(1) “is unique from other provisions of Rule 41 because it implicates substantive judicial authority,” and accordingly concluding that past cases involving violations of other subsections of Rule 41 “offer limited guidance”) (internal quotation marks and citation omitted). Thus, it does not follow from cases involving violations of Rule 41’s procedural provisions that the Rule 41(b) violation at issue here -- which involves the authority of the magistrate judge to issue the warrant, and consequently, the underlying validity of the

---

<sup>10</sup> These violations implicate the various subsections of Rule 41, with the exception of subsection (b). See, e.g., Burgos-Montes, 786 F.3d at 108-09 (magistrate judge’s “failure . . . to define the time period of the search when the form itself provides that the search is to be completed within [10 days], and . . . failure to designate a magistrate to whom the form should be returned” was technical violation of Rule 41(e)); Bonner, 808 F.2d at 869 (officers’ failure to comply with Rule 41(f) requirement of leaving a copy of the warrant at the place to be searched was ministerial and did not call for suppression of resulting evidence); United States v. Dauphinee, 538 F.2d 1, 3 (1st Cir. 1976) (“The various procedural steps required by Rule 41(d) are basically ministerial[,]” and therefore suppression of evidence obtained in violation of that provision was not warranted absent showing of prejudice); United States v. Pryor, 652 F.Supp. 1353, 1365-66, (D. Me. 1987) (violation of Rule 41(c)’s procedural requirements regarding nighttime searches did not call for suppression).

warrant -- was simply ministerial. See United States v. Glover, 736 F.3d 509, 515 (D.C. Cir. 2013) (concluding that a Rule 41(b) violation constitutes a "jurisdictional flaw" that cannot "be excused as a 'technical defect'").

Because the violation here involved "substantive judicial authority" rather than simply "the procedures for obtaining and issuing warrants," Krueger, 809 F.3d at 1115 n.7, the Court cannot conclude that it was merely ministerial; in fact, because Rule 41(b) did not grant her authority to issue the NIT warrant, the magistrate judge was without jurisdiction to do so.<sup>11</sup> The government characterizes Levin's challenge as targeting "the location of the search, not probable cause or the absence of judicial approval." Gov't's Resp. 16. Here, however, because the magistrate judge lacked authority, and thus jurisdiction, to issue the NIT Warrant, there simply was no judicial approval. See United States v. Houston, 965 F.Supp.2d 855, 902 n.12 (E.D. Tenn. 2013) ("A search warrant issued by an individual without

---

<sup>11</sup> For the magistrate judge to have had jurisdiction to issue the warrant under Section 636(a), she must have had authority to do so under Rule 41(b), as the government has pointed to no alternative statutory authority or federal rule that could serve as the basis for such jurisdiction. Moreover, the government's argument regarding courts' inherent authority to issue warrants, see Gov't's Resp. 20-21, does not extend to magistrate judges, whose authority derives from -- and is bounded by -- the specific statutory provisions and rules discussed herein.



legal authority to do so is 'void ab initio'") (quoting United States v. Master, 614 F.3d 236, 241 (6th Cir. 2010)); United States v. Peltier, 344 F.Supp.2d 539, 548 (E.D. Mich. 2004) ("A search warrant signed by a person who lacks the authority to issue it is void as a matter of law.") (citation omitted); cf. State v. Surowiecki, 440 A.2d 798, 799 (Conn. 1981) ("[A] lawful signature on the search warrant by the person authorized to issue it [is] essential to its issuance[,] such that an unsigned warrant is void under state law and confers no authority to act, despite existence of probable cause).

NITs, while raising serious concerns,<sup>12</sup> are legitimate law enforcement tools. Indeed, perhaps magistrate judges should have the authority to issue these types of warrants. See In re Warrant to Search a Target Computer at Premises Unknown, 958 F.Supp.2d at 761 (noting that "there may well be a good reason

---

<sup>12</sup> The Court expresses no opinion on the use of this particular police tactic under these circumstances, but notes that its use in the context of investigating and prosecuting child pornography has given rise to significant debate. See, e.g., The Ethics of a Child Pornography Sting, N.Y. Times, Jan. 27, 2016, <http://www.nytimes.com/roomfordebate/2016/01/27/the-ethics-of-a-child-pornography-sting>. The continuing harm to the victims of this hideous form of child abuse is the distribution of the photographs and videos in which the victims appear. See, e.g., United States v. Kearney, 672 F.3d 81, 94 (1st Cir. 2012) (internal citations omitted). Unlike those undercover stings where the government buys contraband drugs to catch the dealers, here the government disseminated the child obscenity to catch the purchasers -- something akin to the government itself selling drugs to make the sting.

to update the territorial limits of [Rule 41] in light of advancing computer search technology").<sup>13</sup> Today, however, no

---

<sup>13</sup> Whether magistrate judges should have the authority to issue warrants to search property located outside of their districts under circumstances like the ones presented here has been the subject of recent deliberations by the Advisory Committee on Criminal Rules. See Memorandum from Hon. Reena Raggi, Advisory Committee on Criminal Rules, to Hon. Jeffrey S. Sutton, Chair, Committee on Rules of Practice and Procedure ("Raggi Mem.") (May 5, 2014); Letter from Mythili Raman, Acting Assistant Attorney General, to Hon. Reena Raggi, Chair, Advisory Committee on the Criminal Rules ("Raman Letter") (Sept. 18, 2013); cf. 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). As Levin points out in his motion, see Def.'s Mot. 18-19, the following proposed amendment to Rule 41(b) is currently under consideration:

- (6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority 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:
  - (A) the district where the media or information is located has been concealed through technological means; or
  - (B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.

Preliminary Draft of Proposed Amendments to the Federal Rules of Appellate, Bankruptcy, Civil, and Criminal Procedure 337-38 ("Proposed Rule 41 Amendment"), Committee on Rules of Practice and Procedure of the Judicial Conference of the United States (August 2014), <http://www.uscourts.gov/file/preliminary-draft-proposed-amendments-federal-rules-appellate-bankruptcy-civil-and-criminal>.

magistrate judge has the authority to issue this NIT warrant. Accordingly, the warrant here was void.

## 2. Prejudice

Even were the Court to conclude that the Rule 41(b) violation was ministerial, suppression would still be appropriate, as Levin has demonstrated that he suffered prejudice. See Burgos-Montes, 786 F.3d at 109 (a Rule 41 violation "does not require suppression unless the defendant can demonstrate prejudice") (emphasis added); cf. Krueger, 809 F.3d at 1117 (affirming district court's order granting defendant's motion to suppress "[b]ecause [the defendant] met his burden of establishing prejudice and because suppression furthers the purpose of the exclusionary rule by deterring law enforcement from seeking and obtaining warrants that clearly violate Rule

---

Proponents of the amendment contend that it ought be adopted in order "to address two increasingly common situations: (1) where the warrant sufficiently describes the computer to be searched but the district within which that computer is located is unknown, and (2) where the investigation requires law enforcement to coordinate searches of numerous computers in numerous districts." Raman Letter 1.

While the Advisory Committee on Criminal Rules unanimously approved the proposed amendment, Raggi Mem. 5, it has drawn criticism from stakeholders ranging from the American Civil Liberties Union, see Letter from American Civil Liberties Union to Members of the Advisory Committee on Criminal Rules (Oct. 31, 2014), to Google, see Letter from Richard Salgado, Director, Law Enforcement and Information Security, Google Inc., to Judicial Conference Advisory Committee on Criminal Rules (Feb. 13, 2015).

41(b)(1)"). "To show prejudice, defendants must show that they were subjected to a search that might not have occurred or would not have been so abrasive had Rule 41[] been followed."<sup>14</sup>

Bonner, 808 F.2d at 869. Here, had Rule 41(b) been followed, the magistrate judge<sup>15</sup> would not have issued the NIT Warrant, and therefore the search conducted pursuant to that Warrant might

---

<sup>14</sup> Courts outside this district faced with Rule 41(b) violations have considered (and in some cases, adopted) alternative formulations of the prejudice inquiry. See, e.g., Krueger, 809 F.3d at 1116 (evaluating government's proposed prejudice standard, "which would preclude defendants from establishing prejudice in this context so long as the [g]overnment hypothetically could have obtained the warrant from a different federal magistrate judge with warrant-issuing authority under the Rule"); Michaud, 2016 WL 337263 at \*6-7. In Michaud, the court reasoned that the most "sensible interpretation" of the prejudice standard in this context is asking "whether the evidence obtained from a warrant that violates Rule 41(b) could have been available by other lawful means[.]" 2016 WL 337263 at \*6 (emphasis added). This Court respectfully declines to follow the Michaud court's approach, instead adhering to the prejudice standard generally applicable to Rule 41 violations. Cf. Krueger, 809 F.3d at 1116 (rejecting government's proposed prejudice standard, which "would preclude defendants from establishing prejudice in this context so long as the Government hypothetically could have obtained the warrant from a different federal magistrate judge with warrant-issuing authority under the Rule[,]" reasoning that "[w]hen it comes to something as basic as who can issue a warrant, we simply cannot accept such a speculative approach" and that instead the standard "should be anchored to the facts as they actually occurred").

<sup>15</sup> This is not to say that a district judge could not have issued the NIT Warrant, since Rule 41(b) and Section 636(a) bear only on the authority of magistrate judges to issue warrants. See infra Part III(B)(4).

not have occurred.<sup>16</sup> See Krueger, 809 F.3d at 1116 (holding that defendant suffered prejudice as a result of having been subjected to a search that violated Rule 41(b), since that search "might not have occurred because the Government would not have obtained [the warrant] had Rule 41(b)(1) been followed."). Contrast United States v. Scott, 83 F.Supp.2d 187, 203 (D. Mass. 2000) (Rule 41(d) violation did not prejudice defendant, since "the nature of the search would not have changed even if [the defendant] had been given a copy of the warrant prior to the search, as required under the rules); United States v. Jones, 949 F.Supp.2d 316, 323 (D. Mass. 2013) (Saris, C.J.) (law enforcement officer's failure to leave the defendant with a copy of the warrant, as required by Rule 41(f), was not prejudicial).

To rebut Levin's prejudice argument, the government appears to ignore the NIT Warrant altogether, baldly stating that "[w]here there is probable cause, judicial approval, and the computer server which the defendant accessed to view child pornography was physically located in the jurisdiction where the issuing magistrate was located, there can be no prejudice to the

---

<sup>16</sup> It follows from this that the government might not have obtained the evidence it seized pursuant to the Residential Warrant, since the application for that warrant was based on information it acquired through the execution of the NIT Warrant. As the government itself points out, it "had no way to know where the defendant was without first using the NIT[.]" Gov't's Resp. 15.

defendant." Gov't's Resp. 16. Simply put, this is not the standard for determining prejudice, and the government directs the Court to no authority to support its assertion. Moreover, as discussed above, the Rule 41(b) violation here had the effect of vitiating the purported judicial approval so, even by this standard, the government's argument against prejudice must fail.

### **3. Good-Faith Exception**

Finally, the government argues that, even if the NIT Warrant violated the Federal Magistrates Act and Rule 41(b), the Court ought not exclude the evidence seized pursuant to the NIT Warrant because the law enforcement officers here acted in good faith. See Gov't's Resp. 21 (citing United States v. Leon, 468 U.S. 897, 918, 926 (1984)). Whether the good-faith exception applies where a warrant was void is a question of first impression in this Circuit, and an unresolved question more broadly. See Wayne R. LaFave, Search and Seizure: A Treatise on the Fourth Amendment, § 1.3(f) n.60 ("It is unclear whether the [Leon good-faith] rule extends to a warrant 'that was essentially void ab initio' because of 'the issuing court's lack of jurisdiction to authorize the search in the first instance.'") (quoting United States v. Baker, 894 F.2d 1144, 1147 (10th Cir. 1990)). This Court holds that it does not.

In Leon, the Supreme Court held that suppression was unwarranted where evidence was obtained pursuant to a search

warrant that was later determined to be unsupported by probable cause, since the executing officers acted in objectively reasonable reliance on the warrant's validity. See 468 U.S. at 922. In reaching this conclusion, the Supreme Court observed that "[r]easonable minds frequently may differ on the question whether a particular affidavit establishes probable cause, and we have thus concluded that the preference for warrants is most appropriately effectuated by according great deference to a magistrate judge's determination." Id. at 914 (internal quotation marks and citation omitted).

Leon contains not the slightest suggestion, however, that the same deference ought apply when magistrate judges determine their own jurisdiction. Indeed, the Supreme Court's conclusion presupposes that the issuing magistrate judge was authorized to issue the challenged warrant. Cf. United States v. Houston, No. 3:13-09-DCR, 2014 WL 259085 at \*26 n.14 (E.D. Tenn. Jan. 23, 2014) (where a warrant is "void ab initio . . . the [c]ourt never reaches the question of whether the search warrant is supported by probable cause") (internal citation omitted). Moreover, Leon deals explicitly with a "subsequently invalidated warrant," 468 U.S. at 918 (emphasis added), rather than a warrant that was void at the time of its issuance. The latter

raises qualitatively different concerns, as several post-Leon courts have recognized.<sup>17</sup>

Over the years since Leon, the Supreme Court has expanded the good-faith exception to contexts beyond those Leon specifically addressed.<sup>18</sup> None of the Supreme Court's post-Leon good-faith cases, however, involved a warrant that was void ab initio, and therefore none direct the conclusion that the good-

---

<sup>17</sup> Courts interpreting the scope of Leon have repeatedly held or acknowledged in dicta that where evidence is obtained pursuant to a warrant that is void ab initio, the good-faith exception has no application. See, e.g., State v. Wilson, 618 N.W.2d 513, 520 (S.D. 2000) (holding that good-faith exception could not save evidence obtained pursuant to warrant issued by state judge acting outside territorial jurisdiction, since "[a]ctions by a police officer cannot be used to create jurisdiction, even when done in good faith"); State v. Nunez, 634 A.2d 1167, 1171 (R.I. 1993) (stating in dicta that Leon good-faith exception "would be inapplicable to this case because" it involved a warrant issued by a retired judge without authority to do so, and thus was "void ab initio"); Commonwealth v. Shelton, 766 S.W.2d 628, 629-30 (Ky. 1989) (noting in dicta that Leon would not be applicable since "in the case at bar, we are not confronted with a technical deficiency; but rather a question of jurisdiction"); United States v. Vinnie, 683 F.Supp. 285, 288-89 (D. Mass. 1988) (Skinner, J.) (holding Leon's good-faith exception inapplicable since the case involved not the "determination of what quantum of evidence constitutes probable cause" but rather "the more fundamental problem of a magistrate judge acting without subject matter jurisdiction").

<sup>18</sup> Leon, along with its companion case, Massachusetts v. Sheppard, 468 U.S. 981 (1984), "contemplated two circumstances: one in which a warrant is issued and is subsequently found to be unsupported by probable cause and the other in which a warrant is supported by probable cause, but is technically deficient." Vinnie, 683 F.Supp. at 288.



faith exception ought apply to this case.<sup>19</sup> This Court is aware of only one federal circuit court to address the question of whether Leon's good-faith exception applies in these circumstances: the Sixth Circuit. See Master, 614 F.3d 236; United States v. Scott, 260 F.3d 512 (6th Cir. 2001). Scott involved a search warrant issued by a retired judge who lacked authority to do so. 260 F.3d at 513. After holding that such warrant was necessarily void ab initio, id. at 515, the court concluded that, "[d]espite the dearth of case law, we are confident that Leon did not contemplate a situation where a

---

<sup>19</sup> The good-faith exception has been held to apply where officers execute a warrant in reliance on existing law. See Davis v. United States, 131 S. Ct. 2419 (2011) (good-faith exception precluded suppression of evidence obtained through a search incident to arrest that was proper under binding appellate precedent at the time of the search but which was later held to be unlawful); Illinois v. Krull, 480 U.S. 340 (1987) (good-faith exception applied to a warrantless administrative search conducted pursuant to a statute later found to be unconstitutional, where the officer's reliance on the constitutionality of the statute was objectively reasonable). Unlike in those cases, here there was no "intervening change in the law that made the good-faith exception relevant." United States v. Wurie, 728 F.3d 1 (1st Cir. 2013).

The Supreme Court has also applied the good-faith exception in circumstances involving one-off mistakes of fact that implicate the validity of a warrant at the time of its execution. See Herring v. United States, 555 U.S. 135 (2009) (good-faith exception applied to evidence improperly obtained as a result of law enforcement's negligent record-keeping practices); Arizona v. Evans, 514 U.S. 1 (1995) (evidence seized in violation of the Fourth Amendment as a result of a clerical error on the part of court personnel was covered by good-faith exception and thus did not warrant suppression). Here, in contrast, the warrant was void at its inception.

warrant is issued by a person lacking the requisite legal authority." Id.

Nine years later, the Sixth Circuit effectively reversed itself in Master, which involved a warrant issued by a state judge to search property outside his district, which was unauthorized under Tennessee law. 614 F.3d at 239. The court held that the warrant was invalid for the same reason as was the warrant in Scott,<sup>20</sup> id. at 240, but that the good-faith exception to the exclusionary rule applied because Scott's reasoning was "no longer clearly consistent with current Supreme Court doctrine." Id. at 242. In particular, it noted that "[t]he Supreme Court has effectively created a balancing test by requiring that in order for a court to suppress evidence following the finding of a Fourth Amendment violation, 'the benefits of deterrence must outweigh the costs.'" Id. at 243 (quoting Herring v. United States, 555 U.S. 135, 142 (2009)).

The Master court read the Supreme Court's recent good-faith cases too broadly.<sup>21</sup> This Court is persuaded instead by the

---

<sup>20</sup> The difference between the issuer of the warrant in Scott and in Master -- namely, a retired judge with "no authority to approve any warrants," and an active judge with authority to issue warrants within his district, respectively -- was "immaterial" for the purpose of determining whether the warrant was valid. Master, 614 F.3d at 240.

<sup>21</sup> Even in Master, it should be noted, the court acknowledged that the recent Supreme Court cases addressing the

rationale in Scott and cases applying the holding of that decision, see, e.g., United States v. Neering, 194 F.Supp.2d 620 (E.D. Mich. 2002) (warrant issued by an official who was not properly appointed and therefore lacked issuing authority was void, and under Scott, the good-faith exception did not apply). Neither Hudson nor Herring -- both of which the Master court cited in support of its conclusion that Scott's holding is no longer tenable, see 614 F.3d at 242 -- requires the conclusion that the good-faith exception applies to evidence seized pursuant to a warrant that was void ab initio.<sup>22</sup>

---

good-faith exception "do[] not directly overrule our previous decision in Scott." 614 F.3d at 243.

<sup>22</sup> In Hudson, 547 U.S. 586 (2006), the Supreme Court held that suppression was not an appropriate remedy for a violation of the knock-and-announce rule. See id. at 599. In reaching this conclusion, the plurality explicitly distinguished the interests protected by the warrant requirement and the knock-and-announce requirement. See id. at 593. With respect to the warrant requirement, it noted that "[u]ntil a valid warrant has issued, citizens are entitled to shield their persons, houses, papers, and effects . . . from the government's scrutiny[,] and that "[e]xclusion of the evidence obtained by a warrantless search vindicates that entitlement." Id. (internal quotation marks and citations omitted) (emphasis added). As no valid warrant was ever issued here, and the government does not argue that an exception to the warrant requirement applies, exclusion is appropriate.

Herring, too, is distinguishable. There, law enforcement officers executed an arrest warrant that had been rescinded. 555 U.S. at 138. The Supreme Court held that since the mistake was attributable to "isolated negligence attenuated from the arrest" -- specifically, a recordkeeping error -- the good-faith exception to the exclusionary rule applied. Id. at 137. Although that case makes much of the connection between the exclusionary rule and the goal of deterrence and culpability of

Because a warrant that was void at the outset is akin to no warrant at all, cases involving the application of the good-faith exception to evidence seized pursuant to a warrantless search are especially instructive. In United States v. Curzi, 867 F.2d 36 (1st Cir. 1989), the First Circuit declined to "recognize[] a good-faith exception in respect to warrantless searches." Id. at 44.<sup>23</sup> To hold that the good-faith exception is applicable here would collapse the distinction between a voidable and a void warrant. But this distinction is meaningful: the former involves "judicial error," such as "misjudging the sufficiency of the evidence or the warrant

---

law enforcement, see id. at 141-43, it says nothing about whether the same calculus ought apply where there was never jurisdiction to issue a valid warrant in the first place.

<sup>23</sup> While no case has directly disturbed this holding, the First Circuit has since held that the good-faith exception may exempt from exclusion evidence seized pursuant to an unconstitutional warrantless search "'conducted in objectively reasonable reliance on binding appellate precedent[.]'" United States v. Sparks, 711 F.3d 58, 62 (1st Cir. 2013) (quoting Davis, 131 S.Ct. at 2434). Cases like Sparks, though, are readily distinguishable: the officers in Sparks were entitled to rely on circuit precedent indicating that they could conduct the challenged search without a warrant; by contrast, here no binding appellate precedent authorized the officers to undertake the search either without a warrant or pursuant to one that was void at the outset. To determine whether the good-faith exception applied in Sparks, the court asked: "what universe of cases can the police rely on? And how clearly must those cases govern the current case for that reliance to be objectively reasonable?" 711 F.3d at 64. Such questions are wholly inapposite here.

application's fulfillment of the statutory requirements[,]" while the latter involves "judicial authority," i.e., a judge "act[ing] outside of the law, outside of the authority granted to judges in the first place." State v. Hess, 770 N.W.2d 769, 776 (Ct. App. Wis. 2009) (emphasis added); cf. Scott, 260 F.3d at 515 ("Leon presupposed that the warrant was issued by a magistrate or judge clothed in the proper legal authority, defining the issue as whether the exclusionary rule applied to 'evidence obtained by officers acting in reasonable reliance on a search warrant issued by a detached and neutral magistrate but ultimately found to be unsupported by probable cause.'") (quoting Leon, 468 U.S. at 900); State v. Vickers, 964 P.2d 756, 762 (Mont. 1998) (distinguishing Leon and concluding that "[i]f a search warrant is void ab initio, the inquiry stops and all other issues pertaining to the validity of the search warrant, such as whether the purpose of the exclusionary rule is served, are moot."). Were the good-faith exception to apply here, courts would have to tolerate evidence obtained when an officer submitted something that reasonably looked like a valid warrant application, to someone who, to the officer, appeared to have authority to approve that warrant application. Cf. Krueger, 809 F.3d at 1126 (Gorsuch, J., concurring). This Court holds that

such an expansion of the good-faith exception is improvident, and not required by current precedent.<sup>24</sup>

Even were the Court to hold that the good-faith exception could apply to circumstances involving a search pursuant to a warrant issued without jurisdiction, it would decline to rule such exception applicable here. For one, it was not objectively reasonable for law enforcement -- particularly "a veteran FBI agent with 19 years of federal law enforcement experience[,]" Gov't's Resp. 7-8 -- to believe that the NIT Warrant was properly issued considering the plain mandate of Rule 41(b). See Glover, 736 F.3d at 516 ("[I]t is quite a stretch to label the government's actions in seeking a warrant so clearly in violation of Rule 41 as motivated by 'good faith.'"); cf. United States v. McKeever, 894 F.2d 712, 717 (5th Cir. 1990) (good-faith exception did not apply where sheriff "who was the prime mover in obtaining and executing the search . . . knew both that

---

<sup>24</sup> While the exclusionary rule has its detractors, see, e.g., Akhil Reed Amar, Fourth Amendment First Principles, 107 Harv. L. Rev. 757, 785-800 (1994) (arguing that suppression is an "awkward and embarrassing remedy" that is unsupported by the text of the Fourth Amendment), "when a criminal conviction is predicated on a violation of the Constitution's criminal procedure requirements, including the Fourth Amendment, the conviction works an ongoing deprivation of liberty without due process," Richard M. Re, The Due Process Exclusionary Rule, 127 Harv. L. Rev. 1885, 1887 (2014); see also Carol S. Steiker, Second Thoughts About First Principles, 107 Harv. L. Rev. 820, 848-852 (1994).

he had to obtain a warrant from a court of record . . . and that [the issuing judge] was not a judge of a court of record." ).<sup>25</sup> Moreover, even analyzed under Herring, the conduct at issue here can be described as "systemic error or reckless disregard of

---

<sup>25</sup> In its oral argument opposing this motion, Elec. Clerk's Notes, ECF No. 62, the government indicated that the particular officers executing the search cannot be charged with the knowledge that the warrant was issued in violation of the Federal Magistrates Act and Rule 41(b). But it would be incongruous to view these officers' conduct in isolation. As Professor Amsterdam articulated:

[S]urely it is unreal to treat the offending officer as a private malefactor who just happens to receive a government paycheck. It is the government that sends him out on the streets with the job of repressing crime and of gathering criminal evidence in order to repress it. It is the government that motivates him to conduct searches and seizures as a part of his job, empowers him and equips him to conduct them. If it also receives the products of those searches and seizures without regard to their constitutionality and uses them as the means of convicting people whom the officer conceives it to be his job to get convicted, it is not merely tolerating but inducing unconstitutional searches and seizures.

Anthony G. Amsterdam, Perspectives on the Fourth Amendment, 58 Minn. L. Rev. 349, 432 (1974).

constitutional requirements,"<sup>26</sup> 555 U.S. at 147, and the Court thus concludes that suppression is appropriate.<sup>27</sup>

#### 4. Policy Ramifications

Notwithstanding the Court's doctrinal analysis -- which has now concluded -- the Court is mindful of the thorny practical questions this motion raises. The government asserts that to hold that the magistrate judge lacked authority to issue the NIT

---

<sup>26</sup> The Supreme Court does not define "systemic negligence," Herring, 555 U.S. at 144, or "systemic error," id. at 147, and the former, at least, is apparently a new term in the Supreme Court's lexicon, see Wayne R. Lafave, The Smell of Herring: A Critique of the Supreme Court's Latest Assault on the Exclusionary Rule, 99 J. Crim. L. & Criminology 757, 784 (2009). It is difficult to ascertain the frequency with which similar warrants -- i.e., warrants to conduct remote searches of property located outside a magistrate judge's judicial district -- are granted, since these warrants are typically issued and remain under seal. See Owsley, supra note 4, at 4-5. Nonetheless, it is clear to the Court that this is far from the sole instance in which the government has sought and obtained an NIT warrant. See id. (listing cases involving NIT warrants or similar); Gov't's Resp. 23.

<sup>27</sup> The Court acknowledges that suppression is an extreme remedy, and consequently it considered whether, on this occasion -- but never again under these circumstances -- the evidence at issue ought be let in under the good-faith exception. See State v. Hardy, No. 16964, 1998 WL 543368, at \*6-7 (Ct. App. Ohio Aug. 28, 1998) (Fain, J., concurring in the judgment) (concluding that good-faith exception should apply to evidence obtained pursuant to a warrant issued without proper jurisdiction, but noting that "[o]nce we allow time for reasonable police officers within this jurisdiction to become acquainted with the territorial limits upon a magistrate judge's authority to issue search warrants, however, claims of good-faith exceptions to the warrant requirement are likely to be unavailing."). Upon further deliberation, however, the Court concluded that to hold that Leon's good-faith exception applies here, where there never existed a valid warrant, would stretch that exception too far.



Warrant, and accordingly to suppress the evidence obtained pursuant thereto, would create "an insurmountable legal barrier" to law enforcement efforts in this realm. Gov't's Resp. 16. The Court is unmoved by the government's argument for two reasons.

First, it cannot fairly be said that the legal barrier to obtaining this type of NIT Warrant from a magistrate judge is "insurmountable," because the government itself has come up with a way of surmounting it -- namely, to change Rule 41(b), see supra note 13.

Second, it does not follow from this opinion that there was no way for the government to have obtained the NIT Warrant. Section 636(a) and Rule 41(b) limit the territorial scope of magistrate judges -- they say nothing about the authority of district judges to issue warrants to search property located outside their judicial districts. Indeed, the quotation from United States v. Villegas, 899 F.2d 1324 (2d Cir. 1990), included in the government's own brief, is revealing: "Rule 41 does not define the extent of the court's power to issue a search warrant. . . . Given the Fourth Amendment's warrant requirements and assuming no statutory prohibition, the courts must be deemed to have inherent power to issue a warrant when the requirements of that Amendment are met." Gov't's Resp. 20-21 (quoting Villegas, 899 F.2d at 1334). With respect to

district judges, neither Rule 41(b) nor Section 636(a) of the Federal Magistrates Act restricts their inherent authority to issue warrants consistent with the Fourth Amendment. See Krueger, 809 F.3d at 1125 n.6 (noting that analysis of a magistrate judge's lack of statutory authority to issue warrants to search outside his district has no bearing on "the statutory authorities of a district judge to issue a warrant for an out-of-district search[,] and pointing out that "[u]nlike magistrates, the jurisdiction of district courts is usually defined by subject matter and parties rather than strictly by geography."); cf. Matter of Application and Affidavit for a Search Warrant, 923 F.2d 324, 326 (4th Cir. 1991) (contrasting a district judge's "inherent power" with a magistrate's power, which is either delegated by a district judge or expressly provided by statute).<sup>28</sup>

---

<sup>28</sup> Surprisingly, a number of courts have apparently understood Rule 41(b) to apply to district judges. See, e.g., United States v. Golson, 743 F.3d 44, 51 (3d Cir. 2014) ("Rule 41(b) grants the authority to issue search warrants to federal judges and judges of state courts of record."); Glover, 736 F.3d at 515 (concluding that a warrant issued by a district judge to search property outside that judge's district violated Rule 41(b)(2)); cf. United States v. Krawiec, 627 F.2d 577, 580 (1st Cir. 1980) (indicating that all "federal warrants" are required to comply with Rule 41). On its face, however, Rule 41(b) applies only to "a magistrate judge" and "a judge of a state court of record." The authority of district judges to issue warrants arises elsewhere, see Villegas, 899 F.2d at 1334; 18 U.S.C. § 3102, and district judges are not subject to the limitations set forth in Rule 41(b).

The magistrate judge who issued this warrant sits primarily in Alexandria, Virginia. See NIT Warrant. Four district judges and three senior judges sit routinely in that courthouse. See Alexandria Courthouse, United States District Court Eastern District of Virginia, <http://www.vaed.uscourts.gov/locations/alex.htm> (last visited Apr. 20, 2016). Here, the government had already involved one of those district judges in its investigation, albeit to obtain the Title III warrant. See Title III Warrant.

Of course, were the government to present its NIT Warrant application to a district judge, it would still have to meet the requirements of the Fourth Amendment, which guarantees that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched.” U.S. Const. amend. IV. Of special concern here is the particularity requirement, since, as the government points out, “the defendant’s use of the Tor hidden service made it impossible for investigators to know what other districts, if any, the execution of the warrant would take place in,” Gov’t’s Resp. 20.<sup>29</sup> While this Court need not decide whether the

---

<sup>29</sup> Indeed, objectors to the proposed amendment to Rule 41(b), see supra note 13, have argued that a warrant that permitted law enforcement to remotely search computers at unknown locations would violate the Fourth Amendment’s particularity requirement. See, e.g., Written Statement of the

particularity requirement was met here, it notes that despite the difficulty highlighted by the government, at least two courts have determined that this precise warrant was sufficiently particular to pass constitutional muster. See United States v. Epich, No. 15-CR-163-PP, 2016 WL 953269, at \*2 (E.D. Wis. Mar. 14, 2016); United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263 at \*4-\*5 (W.D. Wash. Jan. 28, 2016). But cf. In re Warrant to Search a Target Computer at Premises Unknown, 958 F.Supp.2d at 755-58 (warrant to "surreptitiously install[] software designed . . . to extract certain stored electronic records" from "an unknown computer at an unknown location" did not satisfy Fourth Amendment particularity requirement).

#### **IV. CONCLUSION**

Based on the foregoing analysis, the Court concludes that the NIT Warrant was issued without jurisdiction and thus was void ab initio. It follows that the resulting search was conducted as though there were no warrant at all. Since warrantless searches are presumptively unreasonable, and the good-faith exception is inapplicable, the evidence must be excluded. Accordingly, Levin's motion to suppress, ECF No. 44, is GRANTED.

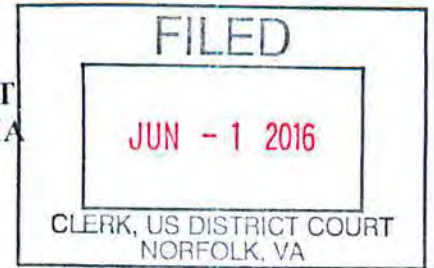
---

Center for Democracy & Technology Before the Judicial Conference Advisory Committee on Criminal Rules 2, Oct. 24, 2014.

SO ORDERED.

/s/ William G. Young  
WILLIAM G. YOUNG  
DISTRICT JUDGE

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



UNITED STATES of AMERICA,

v.

Criminal No. 4:16cr16

\*\*UNDER SEAL\*\*

EDWARD JOSEPH MATISH, III,

Defendant.

OPINION & ORDER

This matter is before the Court on Defendant Edward Matish, III's ("Defendant" or "Matish") First Motion to Suppress ("First Motion"), Doc. 18, and Third Motion to Suppress ("Third Motion"), Doc. 34. Trial in this case is scheduled for June 14, 2016.

On February 8, 2016, Defendant was named in a four (4) count criminal indictment charging him with access with intent to view child pornography, in violation of 18 U.S.C. § 2252A(a)(5) and (b)(2). Doc. 1. The Government filed an eight (8) count superseding indictment on April 6, 2016, charging Defendant with access with intent to view child pornography, in violation of 18 U.S.C. § 2252A(a)(5) and (b)(2) (Counts One through Four), and receipt of child pornography, in violation of 18 U.S.C. § 2252A(a)(2) and (b)(1) (Counts Five through Eight). Doc. 26. Defendant filed his First Motion on March 17, 2016, Doc. 18, and he adopted it after the Government filed the superseding indictment on April 8, 2016, Doc. 30. Defendant filed his Third Motion on May 2, 2016. Doc. 34.

In the Motions, Defendant seeks to suppress "all evidence seized from Mr. Matish's home computer by the FBI on or about February 27, 2015 through the use of a network investigative technique, as well as all fruits of that search." Doc. 18 at 1; Doc. 34 at 1.

Defendant challenges the warrant authorizing the search on the grounds that it lacked probable cause, that the FBI included false information and omitted material information in the supporting affidavit intentionally or recklessly, that the warrant lacked specificity, and that the warrant's triggering event never occurred. See Doc. 18; Doc. 33. Defendant also argues that the warrant was void *ab initio*, making the warrantless search unconstitutional. Doc. 34 at 1. Finally, Defendant "alleges a prejudicial and deliberate violation of Rule 41." Id.

Other courts across the country have considered various challenges to the particular warrant used in this case. See United States v. Michaud, No. 3:14-cr-05351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016); United States v. Stamper, No. 1:15-cr-109, ECF No. 48 (S.D. Ohio Feb. 19, 2016); United States v. Levin, No. 15-10271, 2016 WL 2596010 (D. Mass. Apr. 20, 2016); United States v. Arterbury, No. 15-cr-182, ECF No. 47 (N.D. Okla. Apr. 25, 2016) (adopting the report and recommendation of a magistrate judge, ECF No. 42); United States v. Werdene, No. 2:15-cr-00434, ECF No. 33 (E.D. Pa. May 18, 2016); United States v. Epich, No. 15-cr-163, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016).

The Court held hearings to address these Motions on May 19, 2016 and May 26, 2016. The Court **FINDS**, for the reasons stated herein, that probable cause supported the warrant's issuance, that the warrant was sufficiently specific, that the triggering event occurred, that Defendant is not entitled to a Franks hearing, and that the magistrate judge did not exceed her jurisdiction or authority in issuing the warrant. Furthermore, the Court **FINDS** that suppression is not warranted because the Government did not need a warrant in this case. Thus, any potential defects in the issuance of the warrant or in the warrant itself could not result in constitutional violations, and even if there were a defect in the warrant or in its issuance, the good faith

exception to suppression would apply. Therefore, the Court **DENIES** Defendant's First and Third Motions to Suppress.

## I. FACTUAL BACKGROUND

The prosecution of Mr. Matish stems from the Government's investigation of Playpen, a website that contained child pornography. At the hearing on May 19, 2016, the Court heard testimony from FBI Special Agents Daniel Alfin and Douglas Macfarlane. The Court also admitted several Defense Exhibits. See Def. Exs. 1A, 1B, 2, 3, 4, 5, 6. Doc. 58. The Court admitted Ex. 5 under seal. Id. Additionally, the Court received a brief of amicus curiae from the Electronic Frontier Foundation. See Doc. 42. These sources, in addition to the parties' briefs, informed the Court's understanding of the relevant facts, which are recounted below.

### *i. The Tor Network*

Playpen operated on "the onion router" or "Tor" network. The U.S. Naval Research Laboratory created the Tor network in an attempt to protect government communications. The public now can access the Tor network. Many people and organizations use the Tor network for legal and legitimate purposes; however, the Tor network also is replete with illegal activities, particularly the online sexual exploitation of children.

A person can download the Tor browser from the Tor website. See Tor, <https://www.torproject.org> (last visited May 23, 2016). SA Alfin testified that the Tor network possesses two primary purposes: (1) it allows users to access the Internet in an anonymous fashion and (2) it allows some websites – hidden services – to operate only within the Tor network. Although a website's operator usually can identify visitors to his or her site through the visitors' Internet Protocol ("IP") addresses, a Tor user's IP address remains hidden. Additionally, people who log into a hidden service cannot identify or locate the website itself.



Furthermore, all communications on hidden services are encrypted. Thus, the Tor network provides anonymity protections to both operators of a hidden service and to visitors of a hidden service. There exist index websites of Tor hidden services that users can search, although these indexes behave differently than a typical search engine like Google. According to SA Alfin, there are more than 1,000 servers all over the world in the Tor network. Because Tor users' IP addresses remain hidden, the Government cannot rely on traditional identification techniques to identify website visitors who utilize the Tor network.

*ii. Playpen*

Both parties agree that Playpen contained child pornography. While SA Alfin described Playpen as being entirely dedicated to child pornography, Doc. 59 at 51–52, the Government conceded in its briefs that some of Playpen's sections and forums did not consist entirely of child pornography. See Doc. 24 at 11 (noting that the “vast majority” of Playpen's sections, forums, and sub-forums were “categorized repositories for sexually explicit images of children, subdivided by gender and the age of the victims”). The Government characterizes Playpen as a hidden service, but Defendant disputes that Playpen always resembled a hidden service, claiming that “due to an error in Playpen's connections with the Tor network, it could be found and viewed on both the Tor network and the regular Internet for at least part of the time that it was operating.” Doc. 18 at 5.

The Government notes that the “scale of child sexual exploitation on the site was massive: more than 150,000 total members created and viewed tens of thousands of postings related to child pornography.” Doc. 24 at 4. Additionally, “[i]mages and videos shared through the site were highly categorized according to victim age and gender, as well as the type of sexual activity. The site included forums for discussion of all things related to child sexual exploitation,

including tips for grooming victims and avoiding detection.” *Id.* at 4. The victims displayed on Playpen were both foreign and domestic, and some represent children known to the Government. Upon registering for an account with Playpen, potential users were warned not to enter a real email address or post identifying information in their profiles.

In December 2014, a foreign law enforcement agency discovered Playpen and alerted the FBI. After locating Playpen’s operator, the FBI executed a search of his home in Florida on February 19, 2015, seizing control of Playpen. The FBI did not immediately shut Playpen down; instead, it assumed control of Playpen, continuing to operate it from a government facility in the Eastern District of Virginia from February 20, 2015 through March 4, 2015. As of February 20, 2015, Playpen had 158,094 members from all over the world, 9,333 message threads, and 95,148 posted messages. Doc. 18 at 6; Doc. 24 at 9. Defendant argues a substantial increase in the usage of Playpen occurred after the Government took it over. While the Government concedes that there was some increase, it disputes the unsupported figures in Defendant’s briefs.

*iii. The NIT Warrant and the Supporting Affidavit*

On February 20, 2015, an experienced and capable federal magistrate judge authorized the FBI to deploy a network investigative technique (“NIT”) on Playpen’s server to obtain identifying information from activating computers, which the warrant defines as computers “of any user or administrator who logs into [Playpen] by entering a username and password.” Def. Ex. 1A. It is undisputed that the FBI could not identify the locations of any of the activating computers prior to deploying the NIT. The NIT is a set of computer instructions or computer code that in this case instructed an activating computer to send certain information to the FBI. This information included:

1. the activating computer’s IP address, and the date and time that the NIT determines what that IP address is;

2. a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish data from that of other activating computers, that will be sent with and collected by the NIT;
3. the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86);
4. information about whether the NIT has already been delivered to the activating computer;
5. the activating computer's Host Name;
6. the activating computer's active operating system username; and
7. the activating computer's media access control ("MAC") address.

Def. Ex. 1A. In order to determine a target's location, the FBI only needed to identify the first piece of information described above. SA Macfarlane acted as the affiant, and he signed the warrant application. SA Macfarlane has nineteen (19) years of federal law enforcement experience.

The NIT Warrant application described Playpen's home page logo as depicting "two images [of] partially clothed prepubescent females with their legs spread apart, along with the text underneath stating, 'No cross-board reposts, .7z preferred, encrypt filenames, include preview, Peace out.'" Def. Ex. 1B ¶ 12. This description was inaccurate at the time the magistrate judge signed the warrant, although SA Macfarlane did not know of the inaccuracies at the time he sought the magistrate's authorization. A very short time before the FBI assumed control of Playpen, the logo changed from depicting two partially clothed prepubescent females with their legs spread apart to displaying a single image of a female. SA Alfin described this image as "a single prepubescent female wearing fishnet stockings and posed in a sexually suggestive manner." Doc. 59 at 33. The text underneath the logo remained unchanged. SA Alfin participated in the search of Playpen's operator's home in Florida, and he testified that during the search he saw the website displayed on the operator's computer. However, though SA Alfin admits to viewing the new logo, he testified that "it went unobserved by me because it was an insignificant change to the Web site." Doc. 59 at 10.

Even though the warrant authorized the FBI to deploy the NIT as soon as a user logged into Playpen, SA Alfin testified that the Government did not deploy the NIT against Mr. Matish in this particular case until after someone with the username of “Broden” logged into Playpen, arrived at the index site, went to the bestiality section – which advertised prepubescent children engaged in sexual activities with animals – and clicked on the post titled “Girl 11YO, with dog.” In other words, the agents took the extra precaution of not deploying the NIT until the user first logged into Playpen and second entered into a section of Playpen which actually displayed child pornography. At this point, testified SA Alfin, the user downloaded several images of child pornography as well as the NIT to his computer. Thus, the FBI deployed the NIT in a much narrower fashion than what the warrant authorized.

After determining a user’s IP address via the NIT, the FBI can send a subpoena to an Internet Service Provider (“ISP”), which will be able to identify the computers that possessed that IP address on a particular date and time. Based on this information, a different experienced and capable magistrate judge authorized a residential search warrant for Mr. Matish’s home, which the FBI executed on July 29, 2015. Pursuant to this second warrant, the FBI seized several computers, hard drives, cell phones, tablets, and video game systems.

## **II. Probable Cause Supported the Issuance of the NIT Warrant**

### **A. Legal Standards**

The Fourth Amendment to the United States Constitution provides that “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. As the Supreme Court of the United

States noted in Illinois v. Gates, “probable cause is a fluid concept – turning on the assessment of probabilities in particular factual contexts – not readily, or even usefully, reduced to a neat set of legal rules.” 462 U.S. 213, 232 (1983). Therefore, a magistrate considering whether probable cause supports the issuance of a search warrant simply must “make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, including the ‘veracity’ and ‘basis of knowledge’ of persons supplying hearsay information, there is a fair probability that contraband or evidence of a crime will be found in a particular place.” Id. at 238. In order for a magistrate to conclude that probable cause exists, a warrant application’s supporting affidavit must be more than conclusory and bare bones; indeed, the affidavit “must provide the magistrate with a substantial basis for determining the existence of probable cause.” Id. at 239. Probable cause is not subject to a precise definition, and it is a relaxed standard. See United States v. Allen, 631 F.3d 164, 172 (4th Cir. 2011); see also United States v. Martin, 426 F.3d 68, 76 (2d Cir. 2005) (citing United States v. Leon, 468 U.S. 897, 958 (1084)). When examining an affidavit, a magistrate may rely on law enforcement officers who may “draw on their own experience and specialized training to make inferences from and deductions about the cumulative information available to them that might well elude an untrained person,” as long as the affidavit contains facts to support the law enforcement officer’s conclusions. United States v. Johnson, 599 F.3d 339, 343 (4th Cir. 2010) (quoting United States v. Arvizu, 534 U.S. 266, 273 (2002)) (internal quotations omitted); see also United States v. Brown, 958 F.2d 369, at \*5 (4th Cir. 1992) (noting that “magistrates, in making probable cause determinations, may rely upon an experienced police officer’s conclusions as to the likelihood that evidence exists and where it is located”).

A court reviewing whether a magistrate correctly determined that probable cause exists should afford the magistrate's determination of probable cause great deference. See Gates, 462 U.S. at 236. Therefore, "the duty of a reviewing court is simply to ensure that the magistrate had a 'substantial basis for . . . conclud[ing] that' probable cause existed." Id. at 238–39 (quoting Jones v. United States, 362 U.S. 257, 271 (1960)); see also United States v. Blackwood, 913 F.2d 139, 142 (4th Cir. 1990). A reviewing court should "resist the temptation to 'invalidate warrant[s] by interpreting affidavit[s] in a hypertechnical, rather than a commonsense, manner.'" Blackwood, 913 F.2d at 142 (quoting Gates, 462 U.S. at 236).

## **B. Analysis**

Defendant first challenges the NIT Warrant on its face, arguing that it is not based on probable cause, even if the Court were to ignore the warrant application's inaccuracies. See Doc. 18 at 11–12; Doc. 33 at 3. The Government, in contrast, argues that the facts contained in the 31-page affidavit written by a 19-year FBI veteran with specialized training and experience in this field, "along with the reasonable inferences to be drawn therefrom, support probable cause to believe that registered users of Playpen intended to view and trade child pornography." Doc. 24 at 17.

The Court **FINDS** that the magistrate possessed a substantial basis for determining that probable cause existed to support the issuance of the NIT Warrant. Taking the affidavit at face value, it outlines numerous affirmative steps that one must take to find Playpen on the Tor network, it describes Playpen's home page and registration terms in detail, and it details Playpen's content. See Def. Ex. 1B. Examining the totality of these circumstances leads to the conclusion that there existed a fair probability that those accessing Playpen intended to view and trade child pornography and that the NIT would help uncover evidence of crimes.

The affidavit describes the Tor network and its emphasis on anonymity. See Def. Ex. 1B at 10–11. It states that “the TARGET WEBSITE is a Tor hidden service.” Id. ¶ 10. It explains that a user cannot access a hidden service unless he or she knows the particular website address. Id. The affidavit, therefore, describes numerous affirmative steps that one must take even to find Playpen on the Tor network. The Court credits SA Alfin’s testimony that it would be extremely unlikely for someone to stumble innocently upon Playpen. The magistrate thus was justified in concluding that the chances of someone innocently discovering, registering for, and entering Playpen were slim.

Additionally, the affidavit illustrates Playpen’s home page, detailing the picture of the two prepubescent females as well as the text. Id. ¶ 12. The affiant explained that based on his training and experience, he knew that “‘no cross-board reposts’ refers to a prohibition against material that is posted on other websites from being ‘re-posted’ to the TARGET WEBSITE; and ‘.7z’ refers to a preferred method of compressing large files or sets of files for distribution.” Id. ¶ 12. The affidavit also explained that users viewed a warning message upon accessing the “register an account” hyperlink, informing them not to enter a real email address or to post information that could be used to identify oneself. Id. ¶ 13. It also warned that the website “is not able to see your IP . . .” Id. ¶ 13.

In addition, the affidavit described Playpen’s contents. It noted that “the entirety of the TARGET WEBSITE is dedicated to child pornography.”<sup>1</sup> Id. ¶ 27. While Defendant disputes this characterization, it was not unreasonable for the affiant to conclude, or for the magistrate to accept, that the site was indeed dedicated to child pornography. The affidavit also detailed sections, forums, and sub-forums visible upon logging into the site, most of which referenced

---

<sup>1</sup> “Dedicated” to child pornography does not mean that every section actually consisted of child pornography – some forums apparently discussed how to prepare a child and examples of child abuse. This distinction may explain the seeming conflict between SA Alfin’s testimony and the Government’s brief.

children. SA Alfin testified that even the topics listed on the home page that could refer to adult pornography actually referenced child pornography in the context of Playpen. The affiant also noted that he believed users employed Playpen's private message system to disseminate child pornography. Id. ¶ 22. Finally, the affidavit described sub-forums that contained "the most egregious examples of child pornography and/or [were] dedicated to retellings of real world hands on sexual abuse of children." Id. ¶ 27.

Therefore, it was not unreasonable for the magistrate judge to find that Playpen's focus on anonymity, coupled with Playpen's suggestive name, the logo of two prepubescent females partially clothed with their legs spread apart, and the affidavit's description of Playpen's content, endowed the NIT Warrant with probable cause. In fact, other courts have found that probable cause supported this exact NIT Warrant. In Epich, for example, the Eastern District of Wisconsin adopted a magistrate judge's report and recommendation, which "pointed to the complicated machinations through which users had to go to access the web site (meaning that unintentional users were unlikely to stumble onto it); the fact that the web site's landing page contained images of partially clothe[d] prepubescent females with their legs spread apart; the existence of statements on the landing page that made it clear that users were not to re-post materials from other web sites, and provided information for compressing large files (such as video files) for distribution; the fact that the site required people to register to use it, and advised registrants to use fake e-mail addresses and emphasized that the site was anonymous; and the fact that once a user went through all of *those* steps to become a registered user, the user had access to the entire site, which contained images and/or videos that depicted child pornography." 2016 WL 953269, at \*1-2. The court thus concluded that "anyone who ended up a registered user on the web site was aware that the site contained, among other things, pornographic images



of children.” Id. The magistrate judge in Epich additionally found that “the fact that one could become a registered user to the web site, and then view only information that did not contain illegal material, did not affect the probable cause determination that the Virginia magistrate judge made in issuing the warrant.” Id. Similarly, in Michaud, the Western District of Washington stated that “it would be highly unlikely that [Playpen] would be stumbled upon accidentally, given the nature of the Tor network.” 2016 WL 337263, at \*5. Thus, taking the NIT Warrant at its face, the Court **CONCLUDES** that the magistrate judge possessed ample probable cause to issue the NIT Warrant.

### **III. A Franks Hearing is Not Warranted**

#### **A. Legal Standards**

In Franks v. Delaware, the Supreme Court held that if a “defendant makes a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included by the affiant in the warrant affidavit, and if the allegedly false statement is necessary to the finding of probable cause, the Fourth Amendment requires that a hearing be held at the defendant’s request.” 438 U.S. 154, 155–56 (1978). If, at the hearing, “the allegation of perjury or reckless disregard is established by the defendant by a preponderance of the evidence, and, with the affidavit’s false material set to one side, the affidavit’s remaining content is insufficient to establish probable cause, the search warrant must be voided and the fruits of the search excluded to the same extent as if probable cause was lacking on the face of the affidavit.” Id. at 156. However, no hearing is required if after “material that is the subject of the alleged falsity or reckless disregard is set to one side, there remains sufficient content in the warrant affidavit to support a finding of probable cause.” Id. at 172.

Because affidavits supporting search warrants are presumed valid, in order to “mandate an evidentiary hearing, the challenger’s attack must be more than conclusory and must be supported by more than a mere desire to cross-examine.” Id. at 171–72. Therefore, “[t]here must be allegations of deliberate falsehood or of reckless disregard for the truth, and those allegations must be accompanied by an offer of proof.” Id. at 171. The defendant can challenge an affidavit on the ground that the affiant intentionally or recklessly included false statements or on the ground that the affiant omitted material facts with the intent to make, or in reckless disregard of whether the omission made, the affidavit misleading. E.g., United States v. Colkley, 889 F.2d 297, 300 (4th Cir. 1990); see also United States v. Chandia, 514 F.3d 365, 373 (4th Cir. 2008). It is insufficient for the defendant to allege mere negligence on the part of the affiant. Colkley, 889 F.2d at 300. To make the necessary substantial preliminary showing, the defendant seeking a Franks hearing should furnish to the Court affidavits or sworn or otherwise reliable statements or satisfactorily explain their absence. Id. A defendant can make a substantial preliminary showing that a false statement was included in the affidavit with reckless disregard for its truth by showing “that an officer acted with a high degree of awareness of [a statement’s] probable falsity, that is, when viewing all the evidence the affiant must have entertained serious doubts as to the truth of his statements or had obvious reasons to doubt the accuracy of the information he reported.” Miller v. Prince George’s County, MD, 475 F.3d 621, 627 (4th Cir. 2007) (quoting Wilson v. Russo, 212 F.3d 781, 788 (3d Cir. 2000)) (internal quotations omitted).

In order to be material, the falsity or the omission in the affidavit “must do more than potentially affect the probable cause determination: it must be ‘necessary to the finding of probable cause.’” Colkley, 889 F.2d at 301 (citing Franks, 438 U.S. at 156). In Colkley, the Fourth Circuit noted that “the district court need not have held a Franks hearing . . . because

inclusion of the omitted information would not have defeated probable cause.” Id. at 299–300. The Fourth Circuit stressed that the district court misstated the type of materiality Franks required when it held that “the affiant’s omission ‘may have affected the outcome’ of the probable cause determination.” Id. at 301. To determine whether the inaccuracies were necessary to find probable cause, a district court must “excise the offending inaccuracies and insert the facts recklessly omitted, and then determine whether or not the ‘corrected’ warrant affidavit would establish probable cause.” Miller, 475 F.3d at 628; see also Martin, 426 F.3d at 75. To make this determination, courts apply the commonsense, totality-of-the-circumstances analysis articulated in Gates. See Colkley, 899 F.2d at 301–02.

## **B. Analysis**

Defendant alleges that the NIT affidavit contains, at a minimum, recklessly misleading statements and omissions that are material to the probable cause determination, and that, therefore, a Franks hearing is warranted. Doc. 18 at 19. Defendant specifically focuses on “the application’s false description of Playpen’s home page, compounded by highly inaccurate statements about how the Tor network functions and a cloud of misleading technical jargon.” Id. at 23. Defendant further argues that the home page’s false description was highly material to the magistrate’s finding of probable cause. Id. at 20. He claims that the affidavit – if it did so at all – persuaded the magistrate judge that the site’s dedication to child pornography would be apparent to anyone viewing the home page “by including a patently inaccurate description of the homepage.” Id. Importantly, Defendant asserts that the inaccurate home page description was clearly relevant to a finding of probable cause, as evidenced by the allegedly dramatic increase in visitors to Playpen after the home page changed. See Doc. 33 at 12–13. Defendant alleges that the increase in visitors “strongly suggests that many new visitors viewed the revised Playpen

homepage as a typical adult site (and had no trouble finding it by Tor search engine or otherwise)” and that “it seems quite plausible that the different content of the Playpen homepage – the misrepresentation at issue here – significantly affected a potential user’s expectations as to the site’s contents.” Id. The Government admits that there was an increase in usage, but it challenges Defendant’s numbers.

The Court **FINDS** that Defendant has not made a substantial showing to justify a Franks hearing. Although SA Alfin admitted that he saw Playpen as it appeared with the new logo on February 19, 2015, there is no evidence before the Court that SA Alfin ever informed SA Macfarlane of the change in the few hours between the conclusion of the residential search in Florida and SA Macfarlane’s seeking the magistrate’s authorization. The Court also finds that it was not reckless for the affiant not to examine the website one more time on the day he sought the warrant’s authorization, as he had recently examined the website and confirmed that nothing had changed. Therefore, the Court **FINDS** that SA Macfarlane did not act intentionally or with any doubt as to the validity of his affidavit when he brought the warrant to the magistrate judge.

Additionally, the Court **FINDS** that the logo change was not material to the probable cause determination. Although the Court questions what caused the increase in visitors after February 20, 2015, even if the warrant had included the description of the new logo instead of the description of the old logo, probable cause still would have existed. Indeed, SA Alfin described the new logo as depicting “a single prepubescent female wearing fishnet stockings and posed in a sexually suggestive manner.” Doc. 59 at 33. Had SA Alfin or Macfarlane described the new image differently, then perhaps the logo change would have been material. However, the Court posits that replacing “two images depicting partially clothed prepubescent females with their legs spread apart,” Def. Ex. 1B ¶ 12, with an image of “a single prepubescent female

wearing fishnet stockings and posed in a sexually suggestive manner,” Doc. 59 at 33, is not significant. Additionally, the logo change lacks significance because the probable cause rested not solely on the site’s logo but also on the affiant’s description that the entire site was dedicated to child pornography, Playpen’s suggestive name, the affirmative steps a user must take to locate Playpen, the site’s repeated warnings and focus on anonymity, and the actual contents of the site.

The Western District of Washington, in considering similar challenges to the same NIT Warrant, orally denied the defendant’s request for a Franks hearing at a motions hearing. Michaud, 2016 WL 337263, at \*1. In a subsequent opinion denying the defendant’s motion to suppress, the court noted that although SA Alfin saw the newer version of Playpen’s home page, he did not notice the picture changes. Id. at \*3. The court stated that the balance of Playpen’s “focus on child pornography apparently remained unchanged, in SA Alfin’s opinion.” Id. Additionally, the court found that the “new picture also appears suggestive of child pornography, especially when considering its placement next to the site’s suggestive name, Play Pen.” Id.

Therefore, Defendant has not made a substantial preliminary showing that the affiant included the inaccurate description of Playpen’s home page either intentionally or recklessly. Furthermore, even if Defendant had made such a showing, a Franks hearing is not warranted because the logo change was immaterial to the probable cause determination. Thus, the Court **DENIES** Defendant’s request for a Franks hearing.

#### **IV. The NIT Warrant Did Not Lack Specificity**

##### **A. Legal Standards**

The Fourth Amendment to the United States Constitution requires that search warrants particularly describe the place to be searched and the persons or things to be seized. U.S. Const. amend. IV. This requirement of particularity “applies to the warrant, as opposed to the

application or the supporting affidavit submitted by the applicant.” E.g., United States v. Hurwitz, 459 F.3d 463, 470 (4th Cir. 2006). By requiring warrants to state the scope of the proposed search with particularity, the Fourth Amendment “ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.” United States v. Talley, 449 Fed. Appx. 301, 302 (4th Cir. 2011). Additionally, the “Fourth Amendment requires that a warrant be no broader than the probable cause on which it is based.” Id. at 473 (citing United States v. Zimmerman, 277 F.3d 426, 432 (3d Cir. 2002)) (internal quotations omitted).

## **B. Analysis**

Defendant argues that the NIT Warrant is overbroad. Doc. 18 at 23. Defendant basis this argument on the fact that the NIT Warrant authorized the FBI to search any of the tens of thousands of computers that accessed Playpen, regardless of the user’s activities on Playpen. Id. at 23–26. Indeed, the warrant “authorized the FBI to execute searches on a population of potential targets so large that it exceeds the population of Charlottesville, Virginia, and many other small cities.” Id. at 26. Defendant claims that the NIT Warrant did not establish probable cause to search a particular location, because it “purportedly gave the FBI broad discretion in deciding when and against whom to deploy its malware technology.” Id. at 23. Thus, Defendant likens the NIT Warrant to a general warrant. Id. at 24. Defendant analogizes to a case from the Eastern District of Arkansas, in which the court held that:

[W]hen, as in this case, a warrant’s scope is so broad as to encompass “any and all vehicles” at a scene, without naming any vehicle in particular, the probable cause on which it stands must be equally broad. Specifically, the Fourth Amendment requires that the probable cause showing in support of an “any and all vehicles” warrant must demonstrate that, at the time of the search, a vehicle’s mere presence at the target location is sufficient to suggest that it contains contraband or evidence of a crime.

United States v. Swift, 720 F.2d 1048, 1055–56 (E.D. Ark. 2010). According to Defendant, “[h]ere – like the mere presence of a car at the scene of a crime – the Government sought to search users’ computers based on mere entry to the Playpen site even though it was not clear from the homepage that someone merely entering the Playpen site – perhaps for the first time – intended to access child pornography.” Doc. 18 at 25.

The Government contends that the “NIT warrant described the places to be searched – activating computers of users or administrators that logged into Playpen – and the things to be seized – the seven pieces of information obtained from those activating computers – with particularity.” Doc. 24 at 29. The Government asks the Court to “decline the defendant’s invitation to read into the Fourth Amendment a heretofore undiscovered upper bound on the number of searches permitted by a showing of probable cause.” Id. In the Government’s view, the fact that “a warrant authorizes the search of a potentially large number of suspects is an indication, not of constitutional infirmity, but a large number of criminal suspects.” Id. at 35.

As noted in Levin, “NITs, while raising serious concerns, are legitimate law enforcement tools.” 2016 WL 2596010, at \*8. Without deciding the particularity issue presented by the NIT Warrant, the District of Massachusetts noted that of “special concern here is the particularity requirement, since, as the government points out, ‘the defendant’s use of the Tor hidden service made it impossible for investigators to know what other districts, if any, the execution of the warrant would take place in.’” Id. at 15. The court noted, however, that despite this difficulty, “at least two other courts have determined that this precise warrant was sufficiently particular to pass constitutional muster.” Id. (citing Epich, 2016 WL 953269, at \*2; Michaud, 2016 WL 337263, at \*4–5) (emphasis in original).

First, in Michaud, the Western District of Washington considered this very issue. 2016 WL 337263, at \*5. In Michaud, the defendant argued that the NIT Warrant amounted to a general warrant and lacked sufficient specificity; however, the court found that “both the particularity and breadth of the NIT Warrant support the conclusion that the NIT Warrant did not lack specificity and was not a general warrant.” Id. Indeed, the court noted that the NIT Warrant “states with particularity exactly what is to be searched, namely, computers accessing” Playpen. Id. Additionally, the fact that the warrant authorized the FBI to search tens of thousands of potential targets “does not negate particularity, because it would be highly unlikely that [Playpen] would be stumbled upon accidentally, given the nature of the Tor network.” Id. The court further held that the NIT Warrant did not exceed the probable cause on which it was issued. Id.

Similarly, in Epich, the Eastern District of Wisconsin, adopting a magistrate judge’s report and recommendation, rejected the defendant’s particularity challenge to the NIT Warrant. 2016 WL 953269, at \*2 (noting that the warrant “explained who was subject to the search, what information the NIT would obtain, the time period during which the NIT would be used, and how it would be used, as well as bearing attachments describing the place to be search and the information to be seized”).

The Court **FINDS** that the NIT Warrant did not violate the Fourth Amendment’s particularity requirement. The Court also **FINDS** that the warrant was not broader than the probable cause upon which it was based. As discussed above – putting aside the admitted inaccuracies and the Franks issue – there existed a fair probability that anyone accessing Playpen possessed the intent to view and trade child pornography. Therefore, the fact that the FBI could have and did narrow its search in this case is immaterial, since the warrant was based on



probable cause to search any computer logging into the site. While Defendant claims Playpen includes sections and forums which do not actually contain child pornography, the only examples in the record concern ways to approach a child who will be the subject of the pornography and relations between adults and children, thus Agent Alfin’s description of the site as “entirely dedicated to child porn.” Additionally, the warrant explicitly outlined the place to be searched – the computers of any user or administrator who logs into Playpen. Def. Ex. 1A. The warrant also detailed the seven items to be seized. Id. Therefore, the NIT Warrant met the Fourth Amendment’s particularity requirements.

## V. The Triggering Event Occurred

### A. Legal Standards

Anticipatory warrants are “based upon an affidavit showing probable cause that at some future time (but not presently) certain evidence of a crime will be located at a specified place.” United States v. Grubbs, 547 U.S. 90, 94 (2006). Generally, these warrants “subject their execution to some condition precedent other than the mere passage of time – a so-called ‘triggering condition.’” Id. If a warrant is subject to a triggering condition and “the government were to execute an anticipatory warrant before the triggering condition occurred, there would be no reason to believe the item described in the warrant could be found at the searched location; by definition, the triggering condition which establishes probable cause has not yet been satisfied when the warrant is issued.” Id. Thus, it “must be true not only that *if* the triggering condition occurs ‘there is a fair probability that contraband or evidence of a crime will be found in a particular place,’ but also that there is probable cause to believe the triggering condition *will occur.*” Id. at 96–97 (citing Gates, 462 U.S. at 238). However, “the Fourth Amendment does

not require that the triggering condition for an anticipatory search warrant be set forth in the warrant itself.” Id. at 99.

## **B. Analysis**

Defendant contends that the NIT Warrant represents an anticipatory warrant “because it prospectively authorized searches whenever unidentified Playpen visitors signed on to the site, with the ‘triggering event’ for those searches being the act of accessing the site.” Doc. 18 at 26. Defendant argues that merely logging into Playpen did not constitute the triggering event; rather “navigating through the internet homepage *described in the warrant application*” represented the triggering condition. Doc. 33 at 2. Since the warrant application incorrectly described Playpen’s home page logo, Defendant could not log into Playpen via the home page described in the warrant application because that home page no longer existed. Id. at 3. Thus, Defendant argues, “the search conducted here was not authorized by the NIT Warrant.” Id.

The Government notes that Defendant’s “claim that the NIT warrant was void because, as an anticipatory warrant, the ‘triggering event’ never occurred is little more than a rehash of the same probable cause and Franks challenges that have already been addressed.” Doc. 24 at 35–36. The Government contends that the relevant triggering event was “the defendant’s decision to enter his username and password into Playpen and enter the site.” Id. The Government emphasizes that Defendant is not claiming that he never logged into Playpen. Id. at 36. Therefore, the Government contends that the triggering event did, in fact, occur. Id.

Defendant’s argument that the triggering event never occurred is novel, but the Court **FINDS** that logging into Playpen – which the application identified by its URL – represents the relevant triggering event. See Def. Ex. 1A. Thus, the triggering event was not conditional upon the website’s home page logo but upon whether a user or administrator of Playpen logged into

the site, which the warrant identified by its URL. The FBI deployed the NIT here after someone with the username “Broden” logged into Playpen. Thus, the Court **FINDS** that the triggering event did occur.

The Court notes that if it were to rule that logging into Playpen through the home page – exactly as it was described in the application – represented the triggering event, as opposed to ruling that simply logging into the website represented the triggering event, such a ruling would provide operators of websites such as Playpen with incentive to frequently change their home pages’ appearances. While this consideration would not be an issue if the FBI had assumed control over the website prior to obtaining the search warrant – as it had in this case – if the FBI obtained a warrant to search computers logging into a site that the FBI had not yet taken over, the website operator’s ability to change his or her website’s home page at will would always defeat probable cause for this type of anticipatory warrant. Again it should be noted that the Government did not employ the NIT until Defendant took the additional step of clicking on an actual child pornography forum or section within Playpen.

## **VI. Rule 41(b)(4) Authorized the Issuance of the NIT Warrant**

### **A. Legal Standards**

Both Federal Rule of Criminal Procedure 41(b) (“Rule 41(b)”) and Section 636 of the Federal Magistrates Act (“Section 636”) concern the scope of a magistrate judge’s authority. Rule 41(b) details a magistrate judge’s authority to issue a search warrant. See Fed. R. Crim. P. 41(b). It provides that:

- (1) a magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district;
- (2) a magistrate judge with authority in the district has authority to issue a warrant for a person or property outside the district if the person or property is located

within the district when the warrant is issued but might move or be moved outside the district before the warrant is executed;

(3) a magistrate judge—in an investigation of domestic terrorism or international terrorism—with authority in any district in which activities related to the terrorism may have occurred has authority to issue a warrant for a person or property within or outside that district;

(4) a magistrate judge with authority in the district has authority to issue a warrant to install within the district a tracking device; the warrant may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both; and

(5) a magistrate judge having authority in any district where activities related to the crime may have occurred, or in the District of Columbia, may issue a warrant for property that is located outside the jurisdiction of any state or district, but within any of the following:

(A) a United States territory, possession, or commonwealth;

(B) the premises—no matter who owns them—of a United States diplomatic or consular mission in a foreign state, including any appurtenant building, part of a building, or land used for the mission’s purposes; or

(C) a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state.

Fed. R. Crim. P. 41(b). Section 636(a) of the Federal Magistrates Act addresses a magistrate judge’s jurisdiction and provides, in relevant part:

(a) Each United States magistrate judge serving under this chapter shall have within the district in which sessions are held by the court that appointed the magistrate judge, at other places where that court may function, and elsewhere as authorized by law—

(1) all powers and duties conferred or imposed upon United States commissioners by law or by the Rules of Criminal Procedure for the United States District Courts . . .

28 U.S.C. § 636. As the District of Massachusetts noted in Levin, “the Court’s analyses of whether the NIT Warrant was statutorily permissible and whether it was allowed under Rule 41(b) are necessarily intertwined.” 2016 WL 2596010, at \*3. Indeed, “[f]or the magistrate judge

to have had jurisdiction to issue the warrant under Section 636(a), she must have had authority to do so under Rule 41(b).” Id. at \*8 n.11.

## **B. Analysis**

### *i. Defendant Has Standing to Challenge the Magistrate Judge’s Authority and Jurisdiction*

In Rakas v. Illinois, the Supreme Court of the United States stressed that “Fourth Amendment rights are personal rights which, like some other constitutional rights, may not be vicariously asserted.” 439 U.S. 128, 133–34 (1978) (quoting Brown v. United States, 411 U.S. 223, 230 (1973)). Therefore, a “person who is aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person’s premises or property has not had any of his Fourth Amendment rights infringed” and thus cannot vicariously assert the third party’s Fourth Amendment rights. Id. at 134. In Rakas, the Supreme Court held that passengers of a car who “asserted neither a property nor a possessory interest in the automobile, nor an interest in the property seized” could not vicariously assert the owner and driver’s potential claims that the search of the car violated the Fourth Amendment. Id. at 130, 148.

The Government argues that Defendant does not have standing to assert these challenges to the NIT Warrant, characterizing his Third Motion as one “regarding how the issuance of the NIT warrant would apply to a third party found outside of the Eastern District of Virginia.” See Doc. 53 at 6.

However, the Government deployed the NIT onto Defendant’s own computer, and Defendant is challenging the warrant that purportedly authorized the Government to search that computer. Thus, Defendant possesses standing to challenge the warrant upon which the Government relied. Cf. United States v. Castellanos, 716 F.3d 828, 846 (4th Cir. 2013)

(detailing ways in which defendants can and cannot establish standing to assert Fourth Amendment claims). This case is readily distinguishable from those holding that defendants cannot assert third parties' Fourth Amendment rights. Unlike the passengers in the car in Rakas, 439 U.S. at 134, Defendant obviously possesses an interest in his own computer, and he thus has standing to contest the NIT Warrant on any grounds he sees fit. As Defendant notes, he challenges the warrant “by demonstrating the invalidity of the warrant that purported to authorize this search.” Doc. 55 at 2. Hence, the Court **CONCLUDES** that Defendant possesses standing to challenge the NIT Warrant under Rule 41(b) and Section 636.

*ii. The Magistrate’s Authority and Jurisdiction*

Defendant argues that the magistrate judge “ignored the clearly established jurisdictional limits set forth in Federal Rule of Criminal Procedure 41” in authorizing the search of computers located anywhere in the world. Doc. 24 at 5–6. Defendant alleges that a warrant issued without authority under Rule 41 necessarily leads to a constitutional violation of Section 636. Doc. 34 at 10; Doc. 55 at 3. The Government contends that Rule 41(b)(1), (2), and (4) support the issuance of the warrant and that a violation of Rule 41 does not automatically result in a constitutional violation. Doc. 53 at 12–16

Several courts have held that the magistrate judge lacked authority and jurisdiction to issue the NIT Warrant used in this case. E.g. Levin, 2016 WL 2596010, at \*7; Arterbury, No. 15-182, ECF No. 47; Michaud, 2016 WL 337263, at \*6; Stamper, No. 1:15-cr-109, ECF No. 48; Werdene, No. 2:15-cr-00434, ECF No. 33. As the Eastern District of Pennsylvania noted in Werdene, “the courts generally agree that the magistrate judge in Virginia lacked authority under Rule 41 to issue the warrant, [but] they do not all agree that suppression is required or even appropriate.” No. 2:15-cr-00434, ECF No. 33 (collecting cases). The Court disagrees with the

other courts that have considered this issue and **FINDS** that the magistrate judge did not exceed her authority under Rule 41(b).

The Court **FINDS** that Rule 41(b)(4) authorized the magistrate judge to issue this warrant. Rule 41(b)(4) endows a magistrate with authority to issue a warrant authorizing the use of a tracking device. Fed. R. Crim. P. 41(b)(4). The tracking device must be installed within the magistrate judge's district, but the warrant "may authorize use of the device to track the movement of a person or property located within the district, outside the district, or both." Id.

The Court recognizes that other courts have held this provision inapplicable to the NIT Warrant. See, e.g., Levin, 2016 WL 2596010, at \*6; see also Michaud, 2016 WL 337263, at \*6 (noting that "If the 'installation' occurred on the government-controlled computer, located in the Eastern District of Virginia, applying the tracking device exception breaks down, because [the defendant] never controlled the government-controlled computer, unlike a car with a tracking device leaving a particular district. If the installation occurred on [the defendant's] computer, applying the tracking device exception again fails, because [the defendant's] computer was never physically located within the Eastern District of Virginia." Id.). However, whenever someone entered Playpen, he or she made "a virtual trip" via the Internet to Virginia, just as a person logging into a foreign website containing child pornography makes "a virtual trip" overseas. Because the NIT enabled the Government to determine Playpen users' locations, it resembles a tracking device. Thus, the NIT Warrant authorized the FBI to install a tracking device on each user's computer when that computer entered the Eastern District of Virginia – the magistrate judge's district. Contrary to the opinion conveyed in Michaud, 2016 WL 337263, at \*6, the installation did not occur on the government-controlled computer but on each individual computer that entered the Eastern District of Virginia when its user logged into Playpen via the

Tor network. When that computer left Virginia – when the user logged out of Playpen – the NIT worked to determine its location, just as traditional tracking devices inform law enforcement of a target’s location. Furthermore, as far as this case is concerned, all relevant events occurred in Virginia. The magistrate judge who issued the warrant thus did so with authority under Rule 41(b)(1)(4).

Because the Court **FINDS** that the magistrate judge complied with Rule 41(b) in issuing this warrant, her actions did not contravene Section 636, because she exercised authority that was “conferred or imposed . . . by the Rules of Criminal Procedure for the United States District Courts.” 28 U.S.C. § 636(a)(1).

**VII. Even if the Magistrate Judge Issued the NIT Warrant Without Authority or Jurisdiction, Suppression Is Not Warranted**

**A. The Government Did Not Need a Warrant to Deploy the NIT**

The Court **FINDS** that no Fourth Amendment violation occurred here because the Government did not need a warrant to capture Defendant’s IP address. Therefore, even if the warrant were invalid or void, it was unnecessary, so no constitutional violation resulted from the Government’s conduct in this case.

*i. Legal Standards*

The Fourth Amendment provides, “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. Const. amend. IV. Although holding that the Fourth Amendment protects a person’s “reasonable expectation of privacy,” the Supreme Court cautioned in Katz v. United States that “the Fourth



Amendment cannot be translated into a general constitutional ‘right to privacy.’” 389 U.S. 347, 349, 360 (1967).

Traditionally, the privacy concerns embedded in the Fourth Amendment only applied to government actors’ physical trespasses. See, e.g., United States v. Jones, 132 S. Ct. 945, 949–50 (2012). The Supreme Court, however, expanded the notion of privacy in Katz, and Justice Harlan in concurrence developed a two-part test, which courts now regularly use to determine whether an action violates the Fourth Amendment: (1) the person must have exhibited an actual (subjective) expectation of privacy, and (2) that expectation must be reasonable. 389 U.S. at 361 (Harlan, J., concurring). Hence, to establish a violation of one’s rights under the Fourth Amendment, a defendant “must first prove that he had a legitimate expectation of privacy in the place searched or the item seized.” United States v. Simons, 206 F.3d 392, 298 (4th Cir. 2000). In order to so prove, the defendant “must show that his subjective expectation of privacy is one that society is prepared to accept as objectively reasonable.” Id. (citing California v. Greenwood, 486 U.S. 35, 39 (1988)).

In Katz, the Supreme Court considered whether a reasonable expectation of privacy exists within an enclosed telephone booth. 389 U.S. at 349. Noting that “the Fourth Amendment protects people, not places,” the Court held that the defendant possessed a reasonable expectation of privacy in the words he uttered while in the telephone booth. Id. at 351, 359. In Smith v. Maryland, however, the Supreme Court distinguished Katz, stressing that “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” Smith v. Maryland, 442 U.S. 735, 744 (1979). In Smith, the Supreme Court held that a defendant possessed no expectation of privacy in the phone numbers he dialed, and that, therefore, the installation and use of a pen register to capture the dialed phone numbers did not constitute a

search. Id. at 745. The Court noted that “[a]ll telephone users realize that they must ‘convey’ phone numbers to the telephone company . . .” Id. at 742. Indeed, regardless of the defendant’s location or of the steps he took to maintain privacy, he “had to convey that number to the telephone company . . .” Id. at 743. Thus, the Government did not need a warrant to use the pen register to capture the phone numbers the defendant dialed. Id. at 745. The Ninth Circuit in United States v. Forrester described the dichotomy between Katz and Smith as “a clear line between unprotected addressing information and protected content information.” 512 F.3d 500, 510 (9th Cir. 2007).

Like information revealed to a third party, “[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.” Katz, 389 U.S. at 351. In California v. Ciraolo, the Supreme Court wrote that the “Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares.” 476 U.S. 207, 213 (1986). The Court continued, “[n]or does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer’s observations from a public vantage point . . .” Id. at 213. Even 1,000 feet above a home represents a “public vantage point” “[i]n an age where private and commercial flight in the public airways is routine.” Id. at 215. The defendant in Ciraolo could not reasonably “expect that his marijuana plants,” which he grew in his fenced-in backyard, “were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet.” Id. at 215. The Court thus held that police officers who used a plane flown above the defendant’s backyard to observe his illegal marijuana plants did not conduct a search in violation of the Fourth Amendment. Id.

Similarly, in Minnesota v. Carter, the Supreme Court considered whether a police officer who peered through a gap in a home's closed blinds conducted a search in violation of the Fourth Amendment. 525 U.S. 83, 85 (1998). Although the Court did not reach this question, id. at 91, Justice Breyer in concurrence determined that the officer's observation did not violate the respondents' Fourth Amendment rights. Id. at 103 (Breyer, J., concurring). Justice Breyer noted that the "precautions that the apartment's dwellers took to maintain their privacy would have failed in respect to an ordinary passerby standing" where the police officer stood. Id. at 104. He specified that whether the officer conducted an illegal search cannot turn "upon 'gaps' in drawn blinds. Whether there were holes in the blinds or they were simply pulled the 'wrong way' makes no difference." Id. at 105. "One who lives in a basement apartment that fronts a publicly traveled street, or similar space, ordinarily understands the need for care lest a member of the public simply direct his gaze downward," he continued. Id. Thus, Justice Breyer may have held peering into a gap in closed blinds a permissible act under the Fourth Amendment. Id. at 103.

*ii. Analysis*

**a. Defendant Has No Expectation of Privacy in His IP Address**

The Court first focuses on the Government's discovery of Defendant's IP address, as the IP address ultimately led the Government to Defendant. Without the IP address, the Government presumably would have been unable to locate Defendant, even if the NIT had provided the FBI with the six other pieces of information seized. Here, the Court **FINDS** that Defendant possessed no reasonable expectation of privacy in his computer's IP address, so the Government's acquisition of the IP address did not represent a prohibited Fourth Amendment search.

Generally, one has no reasonable expectation of privacy in an IP address when using the Internet. See, e.g., Forrester, 512 F.3d at 509–11. This lack of a reasonable expectation of privacy stems from the fact that Internet users “should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.” Id. at 510. The Ninth Circuit noted that “IP addresses are not merely passively conveyed through third party equipment, but rather are voluntarily turned over in order to direct the third party’s servers.” Id.

Even an Internet user who employs the Tor network in an attempt to mask his or her IP address lacks a reasonable expectation of privacy in his or her IP address. Presumably, one using the Tor network hopes for, if not possesses, a subjective expectation of privacy in his or her identifying information. Indeed, Tor markets itself as a tool to “prevent[] people from learning your location . . .” See Tor, <https://www.torproject.org> (last accessed May 24, 2016). However, such an expectation is not objectively reasonable in light of the way the Tor network operates. In United States v. Farrell, researchers operating the Tor nodes observed the IP address of the alleged operator of Silk Road 2.0, a Tor hidden service. No. CR15-029, 2016 WL 705197, at \*1 (W.D. Wash. Feb. 23, 2016). Pursuant to a subpoena, the researchers turned over the information to law enforcement. Id. In finding no violation of the Fourth Amendment, the Western District of Washington noted that “in order for [] prospective user[s] to use the Tor network they must disclose information, including their IP addresses, to unknown individuals running Tor nodes, so that their communications can be directed toward their destinations.” Id. at \*2. The Western District of Washington noted that under “such a system, an individual would necessarily be disclosing his identifying information to complete strangers.” Id. Indeed, the Tor Project itself even warns visitors “that the Tor network has vulnerabilities and that users might

not remain anonymous.” Id. The court concluded that “Tor users clearly lack a reasonable expectation of privacy in their IP addresses while using the Tor network.” Id. The court cautioned, however, that its decision was limited to the fact that the researchers “obtained the defendant’s IP address while he was using the Tor network and [the researchers were] operating nodes on that network, and not by any access to his computer.” Id. Accordingly, a magistrate judge’s report and recommendation in the Northern District of Oklahoma that considered whether Playpen users possessed reasonable expectations of privacy in their IP addresses stated that “[w]ere the IP address obtained from a third-party, the [c]ourt might have sympathy for” the position that the defendant did not possess a reasonable expectation of privacy in it; however, “here the IP address was obtained through use of computer malware that entered Defendant’s home, seized his computer and directed it to provide information that the Macfarlane affidavit states was unobtainable in any other way.” Arterbury, No. 15-cr-182, ECF No. 42.

Other courts, however, have not limited the reasonable expectation of privacy inquiry to whether the FBI acquired a defendant’s IP address by accessing his computer or by obtaining the information from a cooperative third party. E.g. Werdene, No. 2:15-cr-00434, ECF No. 33. For example, in another case involving Playpen, the Eastern District of Pennsylvania found that the defendant “had no reasonable expectation of privacy in his IP address,” because “[a]side from providing the address to Comcast, his internet service provider, a necessary aspect of Tor is the initial transmission of a user’s IP address to a third-party.” Id. The court noted in Werdene that “the type of third-party to which [the defendant] disclosed his IP address – whether a person or an ‘entry node’ on the Tor network – does not affect the [c]ourt’s evaluation of his reasonable expectation of privacy.” Id. Because the defendant “was aware that his IP address had been conveyed to a third party, [] he accordingly lost any subjective expectation of privacy in that

information.” Id. Thus, the Eastern District of Pennsylvania found that since the defendant “did not have a reasonable expectation of privacy in his IP address, the NIT cannot be considered a ‘search’ within the meaning of the Fourth Amendment.” Id. Similarly, the Western District of Washington in Michaud stated that the defendant “ha[d] no reasonable expectation of privacy of the most significant information gathered by deployment of the NIT, [his] assigned IP address, which ultimately led to [his] geographic location.” 2016 WL 337263, at \*7. The Western District of Washington likened the defendant’s IP address to an unlisted telephone number that “eventually could have been discovered.” Id.

It is clear to the Court that Defendant took great strides to hide his IP address via his use of the Tor network. However, the Court **FINDS** that any such subjective expectation of privacy – if one even existed in this case – is not objectively reasonable. SA Alfin testified that when a user connects to the Tor network, he or she must disclose his or her real IP address to the first Tor node with which he or she connects. This fact, coupled with the Tor Project’s own warning that the first server can see “This IP address is using Tor,” destroys any expectation of privacy in a Tor user’s IP address. See Tor, <https://www.torproject.org/docs/faq.html.en> (last accessed May 24, 2016); see also Farrell, 2016 WL 705197, at \*2. And, as the Eastern District of Pennsylvania noted, the fact that the Tor network subsequently bounces users’ IP addresses “from node to node within the Tor network to mask [users’] identit[ies] does not alter the analysis of whether” an expectation of privacy in the IP addresses exists. Werdene, No. 2:15-cr-00434, ECF No. 33.

The Court recognizes that the NIT used in this case poses questions unique from the conduct at issue in Farrell, 2016 WL 705197. In Farrell, the Government never accessed the suspect’s computer in order to discover his IP address, whereas here, the Government deployed a set of computer code to Defendant’s computer, which in turn instructed Defendant’s computer to

reveal certain identifying information. The Court, however, disagrees with the magistrate judge in Arterbury, who focused on this distinction, see No. 15-cr-182, ECF No. 42. As the Court understands it, Defendant’s IP address was not located on his computer; indeed, it appears that computers can have various IP addresses depending on the networks to which they connect. Rather, Defendant’s IP address was revealed in transit when the NIT instructed his computer to send other information to the FBI. The fact that the Government needed to deploy the NIT to a computer does not change the fact that Defendant has no reasonable expectation of privacy in his IP address. See Werdene, No. 2:15-cr-00434, ECF No. 33. Thus, the Government’s use of a technique that causes a computer to regurgitate certain information, thereby revealing additional information that the suspect already exposed to a third party – here, the IP address – does not represent a search under these circumstances. Therefore, the Government did not need to obtain a warrant before deploying the NIT and obtaining Defendant’s IP address in this case, so any potential defects in the warrant or in the issuance of the warrant are immaterial.

**b. Defendant Has No Reasonable Expectation of Privacy in His Computer**

While the Court holds that the use of the NIT, which resulted in the Government’s ultimate capture of Defendant’s IP address, does not represent a prohibited search under the Fourth Amendment, the Court acknowledges that the warrant purported to authorize searches of “activating computers.” See Def. Ex. 1A. Without deploying the NIT to a user’s computer, the Government would not have been able to observe any Playpen user’s IP address. Additionally, the Government obtained the six other pieces of identifying data from users’ computers; unlike its acquisition of the IP addresses, which the FBI observed and captured during transmission of the data, the FBI gathered this additional data directly from suspects’ computers. To be sure, “the appropriate [Fourth Amendment] inquiry [is] whether the individual had a reasonable

expectation of privacy in the area searched, not merely in the items found.” E.g., United States v. Horowitz, 806 F.2d 1222, 1224 (4th Cir. 1986). Thus, the Court will address whether Defendant possessed a reasonable expectation of privacy not only in his IP address but also in his computer, the “place to be searched.” Def. Ex. 1A. The Court **FINDS** that Defendant did not possess a reasonable expectation of privacy in his computer.

Examining the search of computers in the Fourth Amendment context, in 2007, the Ninth Circuit held that a defendant had both a subjective expectation of privacy and an objectively reasonable expectation of privacy in his personal computer, even though the defendant had connected that computer to a network. See United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007). The Ninth Circuit noted that a “person’s reasonable expectation of privacy may be diminished in ‘transmissions over the Internet or email that have already arrived at the recipient.’” Id. (quoting United States v. Lifshitz, 369 F.3d 173, 190 (2d Cir. 2004)). “However, the mere act of accessing a network does not in itself extinguish privacy expectations, nor does the fact that others may have occasional access to the computer.” Id. (citing Leventhal v. Knapek, 266 F.3d 64, 74 (2d Cir. 2001)). The Ninth Circuit stressed that “privacy expectations may be reduced if the user is advised that information transmitted through the network is not confidential and that the systems administrators may monitor communications transmitted by the user.” Id. at 1147 (citing Simons, 206 F.3d at 398). Similarly, in United States v. Bruckner, the Fourth Circuit noted that one has a reasonable expectation of privacy in his password-protected home computer. 473 F.3d 551, 555 (4th Cir. 2007). In Trulock v. Freeh, the Fourth Circuit held that “password-protected files [on a computer] are analogous to [a] locked footlocker inside the bedroom;” thus, the defendant “had a reasonable expectation of privacy in the password-protected computer files.” 275 F.3d 391, 403 (2001). Conversely, in Simons, the Fourth Circuit



found that a government employer's remote searches of an employee's computer did not violate the Fourth Amendment, because, in light of the employer's Internet policy – which stated that the employer would monitor employees' use of the Internet – the remote searches did not constitute prohibited searches under the Fourth Amendment. 206 F.3d at 398. The Fourth Circuit further noted that because the employee “lacked a legitimate expectation of privacy in his Internet use,” he also lacked a reasonable expectation of privacy in his computer's hard drive. Id. at 399.

Here, the NIT was programmed to collect very limited information. Like the pen register in Smith that only captured the numbers dialed, 442 U.S. at 742, the NIT only obtained identifying information; it did not cross the line between collecting addressing information and gathering the contents of any suspect's computer. Cf. Forrester, 512 F.3d at 510. Indeed, the Government obtained a traditional residential search warrant before searching the computer's contents in this case. Plus, Defendant lacked any expectation of privacy in the main piece of information the NIT allowed the FBI to gather – his IP address. E.g., Michaud, 2016 WL 337263, at \*7. Additionally, while the Government could have deployed the NIT as soon as a user logged into Playpen, SA Alfin testified that in this particular case, the FBI took the extra step of not deploying the NIT until after the suspect actually accessed child pornography. These facts support the conclusion that the NIT's deployment does not represent a prohibited search under the Fourth Amendment. Cf. Forrester, 512 F.3d at 511.

Additionally, like the employee in Simons who was put on notice that his computer was not entirely private, 206 F.3d at 398, Defendant here should have been aware that by going on Tor to access Playpen, he diminished his expectation of privacy. The Ninth Circuit found in 2007 that connecting to a network did not eliminate the reasonable expectation of privacy in

one's computer, Heckenkamp, 482 F.3d at 1146–47; however, society's view of the Internet – and our corresponding expectation of privacy not only in the information we post online but also in our physical computers and the data they contain – recently has undergone a drastic shift.

For example, hacking is much more prevalent now than it was even just nine years ago, and the rise of computer hacking via the Internet has changed the public's reasonable expectations of privacy. Cf. Lee Raine, *How Americans balance privacy concerns with sharing personal information: 5 key findings*, PEWRESEARCHCENTER (January 14, 2016), <http://www.pewresearch.org/fact-tank/2016/01/14/key-findings-privacy-information-sharing/> (last accessed May 24, 2016) (reporting that members of a focus group “worried about hackers,” though “some accept that [privacy tradeoffs are] a part of modern life”). Now, it seems unreasonable to think that a computer connected to the Web is immune from invasion. Indeed, the opposite holds true: in today's digital world, it appears to be a virtual certainty that computers accessing the Internet can – and eventually will – be hacked.

In the recent past, the world has experienced unparalleled hacks. For example, terrorists no longer can rely on Apple to protect their electronically stored private data, as it has been publicly reported that the Government can find alternative ways to unlock Apple users' iPhones. See Katie Benner and Eric Lichtblau, *U.S. Says It Has Unlocked iPhone Without Apple*, THE NEW YORK TIMES (March 28, 2016), [http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?\\_r=0](http://www.nytimes.com/2016/03/29/technology/apple-iphone-fbi-justice-department-case.html?_r=0) (last accessed May 24, 2016). In addition to politicians being targets of hacking, see Nicole Gaouette, *Intel chief: Presidential campaigns under cyber attack*, CNN (May 18, 2016), <http://www.cnn.com/2016/05/18/politics/presidential-campaigns-cyber-attack/index.html> (last visited May 19, 2016), Ashley Madison, see Alex Hern, *Ashley Madison hack: your questions answered*, THE GUARDIAN (August 20, 2015),

<https://www.theguardian.com/technology/2015/aug/20/ashley-madison-hack-your-questions> answered (last accessed May 24, 2016); Sony, see Peter Elkind, *Sony Pictures: Inside the Hack of the Century*, FORTUNE (July 1, 2015), <http://fortune.com/sony-hack-part-1/> (last accessed May 24, 2016); Home Depot, see Robin Sidel, *Home Depot's 56 Million Card Breach Bigger Than Target's*, THE WALL STREET JOURNAL (Sept. 18, 2014), <http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571> (last accessed May 24, 2016); Target, see id.; the New York Times, see Nicole Perlroth, *Hackers in China Attacked The Times for Last 4 Months*, THE NEW YORK TIMES (Jan. 30, 2013), <http://www.nytimes.com/2013/01/31/technology/chinese-hackers-infiltrate-new-york-times-computers.html> (last accessed May 24, 2016); a Panamanian law firm, see *Panama Papers: Leak firm Mossack Fonseca 'victim of hack'*, BBC NEWS (April 6, 2016), <http://www.bbc.com/news/world-latin-america-35975503> (last accessed May 24, 2016); and even the United States Government, Associated Press in Washington, *US government hack stole fingerprints of 5.6 million federal employees*, THE GUARDIAN (September 23, 2015), <https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints> (last accessed May 24, 2016), all have experienced hacks that resulted in the compromise of unprecedented amounts of data previously thought to be private. Cases identifying a reasonable expectation of privacy in personal computer files protected with only a password, see Bruckner, 473 F.3d at 554; see also Trulock, 275 F.3d at 403, no longer hold merit, because in 2016 it now appears unreasonable to expect that simply utilizing a password provides any practical protection. E.g., Caitlin Dewey, *It's been six months since the Ashley Madison hack. Has anything changed?*, THE WASHINGTON POST (January 15, 2016), <https://www.washingtonpost.com/news/the-intersect/wp/2016/01/15/its-been-six-months-since-the-ashley-madison-hack-has-anything-changed/> (last accessed May 24, 2016) (noting that

“There was always a chance that the Ashley Madison hack, far from waking people up to the dangers of data breaches, would further normalize them.”). Indeed, it is “doubtlessly easier to dismiss hacks this way, as external inevitabilities that no one can really help, than to go through the trauma and unease of reassessing the way we collectively use the Web.” Id.

Tor users likewise cannot reasonably expect to be safe from hackers. Even if Tor users hope that the Tor network will keep certain information private – just as terrorists seem to expect Apple to keep their data private – it is unreasonable not to expect that someone will be able to gain access. See John W. Little, *Tor and the Illusion of Anonymity*, BLOGS OF WAR (August 6, 2013), <http://blogsofwar.com/tor-and-the-illusion-of-anonymity/> (last accessed May 24, 2016) (describing that the Federal Government discovered a way “to identify the true IP addresses [of] an unknown number to Tor users” and noting that this development “should serve as a huge wake-up call” to people who believe that using Tor endows them with unassailable privacy protections). Notwithstanding the identification difficulties posed by Tor and the machinations one must undergo to access a Tor hidden service, advances in technology continue to thwart Tor’s measures.

Thus, hacking resembles the broken blinds in Carter. 525 U.S. at 85. Just as Justice Breyer wrote in concurrence that a police officer who peers through broken blinds does not violate anyone’s Fourth Amendment rights, id. at 103 (Breyer, J., concurring), FBI agents who exploit a vulnerability in an online network do not violate the Fourth Amendment. Just as the area into which the officer in Carter peered – an apartment – is usually afforded Fourth Amendment protection, a computer afforded Fourth Amendment protection in other circumstances is not protected from Government actors who take advantage of an easily broken system to peer into a user’s computer. People who traverse the Internet ordinarily understand the

risk associated with doing so. Thus, the deployment of the NIT to capture identifying information found on Defendant's computer does not represent a search under the Fourth Amendment, and no warrant was needed.

**B. Even if the Issuance of the Warrant Represented a Nonconstitutional Violation of Rule 41(b), Suppression is Still Unwarranted**

The parties agree that two categories of Rule 41 violations exist: "those involving constitutional violations and all others." Doc. 34 at 10; Doc. 53 at 23; Simons, 206 F.3d at 403. Without a constitutional violation, suppression is warranted "only when the defendant is prejudiced by the violation . . . or when there is evidence of intentional and deliberate disregard of a provision in the Rule." Simons, 206 F.3d at 403.

As discussed above, any potential Rule 41 violation did not result in a violation of Defendant's constitutional rights, for no warrant was needed. Thus, the Government's use of the NIT did not deprive Defendant of his Fourth Amendment rights. The Court here **FINDS** that suppression is not appropriate for any potential nonconstitutional violation of Rule 41(b) either, because Defendant was not prejudiced and there is no evidence of intentional or deliberate disregard of the rule.

Defendant argues that the search conducted pursuant to the warrant would not have occurred had the magistrate judge not issued the warrant, and that, therefore, he has suffered prejudice. Doc. 34 at 14. However, as detailed above, the FBI did not need a warrant to deploy the NIT, so Defendant has not shown prejudice.

Additionally, Defendant has failed to show an intentional or deliberate disregard of Rule 41(b). As the Eastern District of Pennsylvania noted in Werdene, the "warrant was candid about the challenge that the Tor network poses, specifically its ability to mask a user's physical location." No. 2:15-cr-00434, ECF No. 33. The affidavit also specifically stated that the NIT

may be deployed against an “activating computer – wherever located.” Def. Ex. 1B ¶ 46. Thus, the Court **FINDS** that the FBI did not attempt to mislead the magistrate judge in any way as to the locations of the activating computers. Therefore, Defendant has shown neither prejudice nor an intentional violation of Rule 41(b), so even if there were a nonconstitutional violation of Rule 41(b), suppression would be inappropriate.

**VIII. Even if the Government Did Need to Obtain a Warrant, and Even if the NIT Warrant Were Invalid, the Good Faith Exception Applies**

Finally, even if the Government did need to obtain a warrant in order to deploy the NIT, and even if there existed defects in the warrant or in its issuance, the Court **FINDS** that suppression still would be inappropriate.

**A. Legal Standards**

Generally, if a search violates the Fourth Amendment, “the fruits thereof are inadmissible under the exclusionary rule, a judicially created remedy designed to safeguard Fourth Amendment rights generally through its deterrent effect.” United States v. Doyle, 650 F.3d 460, 466 (4th Cir. 2011) (citing United States v. Calandra, 414 U.S. 338, 348 (1974)) (internal quotations omitted). However, because exclusion is so drastic a remedy, it represents a “last resort.” United States v. Stephens, 764 F.3d 327, 335 (4th Cir. 2014). Hence, in Leon, the Supreme Court established a good faith exception to the exclusionary rule. See 468 U.S. at 922. Under this exception, the court need not exclude evidence obtained pursuant to a later-invalidated search warrant if law enforcement’s reliance on the warrant was objectively reasonable. Doyle, 650 F.3d at 467. The Fourth Circuit has noted that there are four circumstances in which the Leon good faith exception will not apply:

- (1) if the magistrate or judge in issuing a warrant was misled by information in an affidavit that the affiant knew was false or would have known was false except for his reckless disregard of the truth;
- (2) if the issuing magistrate wholly abandoned

his judicial role in the manner condemned in Lo-Ji Sales, Inc. v. New York, 442 U.S. 319 (1979); (3) if the affidavit supporting the warrant is so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable; and (4) if under the circumstances of the case the warrant is so facially deficient – i.e., in failing to particularize the place to be searched or the things to be seized – that the executing officers cannot reasonably presume it to be valid.

Id. (citing United States v. DeQuasie, 373 F.3d 509, 519–20 (4th Cir. 2004) (quoting Leon, 468 U.S. at 923)) (internal quotations omitted).

## **B. Analysis**

None of the four exceptions to the Leon good faith exception apply in this case. As the Western District of Washington concluded, “[b]ecause reliance on the NIT Warrant was objectively reasonable, the officers executing the warrant acted in good faith, and suppression is unwarranted.” Michaud, 2016 WL 337263, at \*7. Indeed, an experienced and capable magistrate judge reviewed the warrant application and concluded that there existed probable cause to issue the NIT Warrant. As noted above, the FBI did not intentionally or recklessly mislead the magistrate judge in its quest to obtain the NIT Warrant, either on the scope of the warrant or on the information concerning the logo change. Additionally, it does not appear to the Court that the experienced and capable magistrate judge abandoned her judicial role in issuing this warrant, and the warrant application detailed ample probable cause to support the issuance of the warrant. The affidavit also adequately described the items to be seized and the places to be searched. The FBI agents showed no improper conduct or misjudgment in relying upon the NIT Warrant. Therefore, the Leon good faith exception would apply, even if the NIT’s deployment constituted a search and even if the warrant were deficient in some respect.

## **IX. Balance Considerations and Public Policy**

While the Court **FINDS** that the Government did not need a warrant before deploying the NIT, the Court recognizes the need to balance an individual’s privacy in any case involving

electronic surveillance with the Government's duty of protecting its citizens. Here, the balance weighs heavily in favor of surveillance.<sup>2</sup> The Government should be able to use the most advanced technological means to overcome criminal activity that is conducted in secret, and Defendant should not be rewarded for allegedly obtaining contraband through his virtual travel through interstate and foreign commerce on a Tor hidden service. E.g. Werdene, No. 2:15-cr-00434, ECF No. 33 (noting that the defendant "seeks to 'serendipitously receive Fourth Amendment protection' because he used Tor in an effort to evade detection, even though an individual who does not conceal his IP address does not receive those same constitutional safeguards") (citing United States v. Stanley, 753 F.3d 114, 121 (3d Cir. 2014)). Society thus is unprepared to recognize any privacy interests Defendant attempts to claim as reasonable in his search for pornographic material that the Government has subjected to seldom used regulation through prior restraint, see U.S. Const. amend. I, similar to how businesses dealing with heavily regulated products such as liquor and firearms do not possess reasonable expectations of privacy in their interstate commerce activities. See United States v. Biswell, 406 U.S. 311, 316 (1972); see also Colonnade Catering Corp. v. United States, 397 U.S. 72, 74, 77 (1970). The Court **FINDS** that due to the especially pernicious nature of child pornography and the continuing harm to the victims,<sup>3</sup> the balance between any Tor user's alleged privacy interests and the Government's deployment of a NIT to access very limited identifying information weighs in

---

<sup>2</sup> In Riley v. California, the Supreme Court held that "a warrant is generally required before" searching information on a cell phone, "even when a cell phone is seized incident to arrest." 134 S. Ct. 2473, 2493 (2014). Importantly, the Government had searched the contents of an arrestee's cell phone in Riley, including photographs and videos. Id. at 2481. Here, however, the Government did not use the NIT to view anything beyond limited identifying information. Additionally, as the Eastern District of Michigan noted, Riley "did not generate a blanket rule applicable to any data search of any electronic device in any context." No. 15-20631, 2016 WL 894452, at \*4 (E.D. Mich. Mar. 9, 2016). Instead, the Supreme Court "simply held that application of the search incident to arrest doctrine to [searches of digital data] would untether the rule from the justifications underlying it historically." Id. (internal quotations omitted). Therefore, Riley does not control the Court's decision in this case.

<sup>3</sup> The Court does note, however, that it appears some of the continuing harm in this case occurred because the Government continued operating Playpen, rather than immediately shutting it down. The Court expresses no opinion on this particular police tactic, but it does note that when pictures of children appear online, the harm remains in perpetuity.





1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT TACOMA

UNITED STATES OF AMERICA,  
  
Plaintiff,  
  
v.  
  
JAY MICHAUD,  
  
Defendant.

CASE NO. 3:15-cr-05351-RJB  
  
ORDER DENYING DEFENDANT’S  
MOTIONS TO SUPPRESS  
EVIDENCE

These matters come before the Court on Defendant’s Motion to Suppress Evidence (Dkt. 26) and Defendant’s Second Motion to Suppress Evidence and Motion for *Franks* Hearing (Dkt. 65). The Court has considered the parties’ responsive briefing and the remainder of the file herein, as well as the testimony of FBI Special Agent Daniel Alfin and Christopher Soghoian, Principal Technologist for the Speech and Technology Project at the American Civil Liberties Union, elicited at an evidentiary hearing held on January 22, 2016. Dkt. 47, 69, 90, 94, 111. Having orally denied Mr. Michaud’s motion for a *Franks* hearing (Dkt. 135), the sole issue before the Court, raised by both of Mr. Michaud’s motions, is whether to suppress evidence of what Mr. Michaud argues is fruit of an unreasonable search. At oral argument, the parties agreed

1 that the Court should decide the issue based on the submitted record, as supplemented by the  
2 testimony adduced at the hearing. *See* Dkt. 135.

### 3 I. FACTUAL BACKGROUND

#### 4 a. Website A

5 Mr. Jay Michaud, a resident of Vancouver, Washington, is charged with receipt and  
6 possession of child pornography in violation of 18 U.S.C. §§ 2252(a)(2), (a)(4), (b)(1), and  
7 (b)(2). Dkt. 117. The charges against Mr. Michaud stem from Mr. Michaud's alleged activity on  
8 "Website A," a website that, according to the FBI, was dedicated to the advertisement and  
9 distribution of child pornography. Dkt. 47-5, at ¶¶14-16. Website A was created in August of  
10 2014, and by the time that the FBI shut the site down, on March 4, 2015, Website A had over  
11 200,000 registered member accounts and 1,500 daily visitors, making it "the largest remaining  
12 known child pornography hidden service in the world." Dkt. 47-1, at ¶19; Dkt. 50-1, at ¶3.

13 According to the three warrant applications submitted in this case, the main page of the  
14 site featured a title with the words, "Play Pen." Dkt. 47-1, at ¶¶12. *See also* Dkt. 47-5, at ¶¶18-  
15 37; Dkt 47-2, at ¶¶11-21. *See also* Dkt. 90-1, at 2. The main page, which required users to login  
16 to proceed, also featured "two images depicting partially clothed prepubescent females with their  
17 legs apart." *Id.* Text on the same page read, "No cross-board reposts, .7z preferred, encrypt  
18 filenames, include preview, Peace out." *Id.* "No cross-board reposts," appeared to prohibit the  
19 reposting of material from other websites, while ".7z preferred," referred to a preferred method  
20 of compressing large files. *Id.* After logging in, registered users would next view a page with  
21 hyperlinks to forum topics, the clear majority of which advertise child pornography. *Id.*, at ¶¶14-  
22 18. *See also* Dkt. 65-2, at 1-4.

#### 23 b. The Title III Warrant

24

1 On February 20, 2015, agents from the Federal Bureau of Investigation executed a Title  
2 III warrant to intercept the communications of Website A. Dkt. 47-5, at ¶4 and pp. 57-62.  
3 Website A operated on the Tor network, a publicly available alternative internet service that  
4 allows users to mask identifying information, such as Internet Protocol (“IP”) addresses. *Id.*, at  
5 ¶¶18-36. For approximately 14 days, from February 20, 2015 through March 4, 2015, the FBI  
6 administered Website A from a government-controlled computer server located in Newington,  
7 Virginia, which forwarded a copy of all website communications, through the server, to FBI  
8 personnel in Linthicum, Maryland. Dkt. 47-1, at ¶30; Dkt. 47-5, ¶¶38, 52 and p. 60. Based on the  
9 authority of the Title III warrant, the FBI captured communications of users accessing Website  
10 A, including user “Pewter.” The FBI apparently did not post any new content but allowed  
11 registered users to access the site and to continue to post content. *See id.*

12 *c. The NIT Warrant*

13 While controlling Website A, the FBI sought to identify the specific computers, and  
14 ultimately the individuals, accessing the site, by deploying a network investigating technology  
15 (“NIT”) that “cause(d) an activating computer—wherever located—to send to a computer  
16 controlled by or known to the government, network level messages containing information that  
17 may assist in identifying the computer, its location, [and] other information[.]” Dkt. 47-1, at 34.  
18 Prior to deploying the NIT, on February 20, 2015 the FBI sought and obtained a warrant (“the  
19 NIT Warrant”), which was issued by a magistrate judge in the Eastern District of Virginia. *Id.*  
20 The NIT Warrant cover sheet reads as follows:

21 “An application by a federal law enforcement officer . . . requests the search of  
22 the following person of property located in the Eastern District of  
Virginia (*identify the person or describe the property to be searched and give its*  
*location*):

23 See Attachment A

1 The person or property to be searched, described above, is believed to conceal  
(*identify the person or describe the property to be seized*):  
2 See Attachment B[.]” Dkt. 47-1, at 39.

3 Attachment A reads as follows:

4 Attachment A

5 Place to be Searched

6 This warrant authorizes the use of a network investigative technique (“NIT”) to be  
7 deployed on the computer server described below, obtaining information described in  
8 Attachment B from the activating computers below.

9 The computer server is the server operating the Tor network child pornography  
10 website referred to herein as the TARGET WEBSITE, as identified by its URL –  
11 [omitted]— which will be located at a government facility in the Eastern District of  
12 Virginia.

13 The activating computers are those of any user or administrator who logs into the  
14 TARGET WEBSITE by entering a username and password. The government will not  
15 employ this network investigative technique after 30 days after this warrant is authorized,  
16 without further authorization. *Id.*, at 37.

17 Attachment B reads as follows:

18 Attachment B

19 Information to be Seized

20 From any “activating” computer described in Attachment A:

- 21 1. the “activating” computer’s actual IP address, and the date and time that the  
22 NIT determines what that IP address is;  
23  
24

- 1 2. a unique identifier generated by the NIT (e.g., a series of numbers, letters,  
2 and/or special characters) to distinguish data from that other “activating”  
3 computers, that will be sent with and collected by the NIT;
- 4 3. the type of operating system running on the computer, including type (e.g.,  
5 Windows), version (e.g., Windows 7), and architecture (e.g., x 86);
- 6 4. information about whether the NIT has already been delivered to the  
7 “activating” computer;
- 8 5. the “activating” computer’s Host Name;
- 9 6. the “activating” computer’s active operating system username; and
- 10 7. the “activating” computer’s media access control (“MAC”) address;
- 11 that is evidence of violations of . . . [child pornography-related crimes]. *Id.*, at 38.

12 Both Attachment A and Attachment B, which the NIT Warrant incorporated, are identical in  
13 content to the attachments submitted in the warrant application. *Id.*, at 4, 5, 37, 38.

14 *d. Warrant issued in the Western District of Washington (“the Washington Warrant”)*

15 After obtaining the NIT warrant, the FBI deployed the NIT, obtaining the IP address and  
16 other computer-related information connected to a registered user, “Pewter,” who allegedly  
17 accessed Website A for 99 hours between October 31, 2014 and March 2, 2015. Dkt. 47-2, at  
18 ¶26. “Pewter” had apparently accessed 187 threads on Website A, most related to child  
19 pornography. *Id.*, at ¶27. With the IP address in hand, the FBI ultimately ascertained the  
20 residential address associated with “Pewter,” an address at which Mr. Michaud resided, in  
21 Vancouver, Washington. *Id.*, at ¶¶35, 36. A magistrate judge in the Western District of  
22 Washington issued a warrant to search that address, and the FBI subsequently seized computers  
23 and storage media allegedly containing contraband. *See generally, id.*

1 *e. Evidentiary testimony of SA Alfin and Dr. Christopher Soghoian*

2 SA Alfin's testimony explained how the NIT was deployed against Mr. Michaud. While  
3 the FBI administered Website A from a government-controlled computer, between February 20,  
4 2015 and March 4, 2015, a registered user, "Pewter," logged into Website A and accessed a  
5 forum entitled, "Preteen videos—girls HC." (HC stands for "hardcore.") The FBI setup the NIT  
6 so that accessing the forum hyperlink, not Website A's main page, triggered the automatic  
7 deployment of the NIT from the government-controlled computer in the Eastern District of  
8 Virginia, to Pewter's computer in Vancouver, Washington, where the NIT collected the IP  
9 address, MAC address, and other computer-identifying information, and relayed that information  
10 back to the government-controlled server in the Eastern District of Virginia, after which the  
11 information was forwarded to FBI personnel for data analysis.

12 SA Alfin also explained a discrepancy in the content of Website A's main page. While  
13 the warrant application for the NIT describes a main page featuring two prepubescent females  
14 with legs spread apart, Dkt. 47-1, at ¶12, by the time that the FBI submitted the warrant  
15 application, on February 20, 2015, the main page had been changed to display only one young  
16 female with legs together. *Compare* Dkt. 90-1, at 2 and Dkt. 90-1, at 4. According to SA Alfin,  
17 the main page changed several hours prior to the arrest of a Website A administrator, in the early  
18 evening hours of February 19, 2015. After the arrest, SA Alfin viewed Website A and other  
19 material on the administrator's computer, at which point SA Alfin saw the newer version of  
20 Website A's main page but did not notice the picture changes. The balance of Website A's focus  
21 on child pornography apparently remained unchanged, in SA Alfin's opinion. The new picture  
22 also appears suggestive of child pornography, especially when considering its placement next to  
23 the site's suggestive name, Play Pen.

1 Dr. Christopher Soghoian, testifying on behalf of Mr. Michaud, explained how the Tor  
2 network functions and theorized about how the NIT may have been deployed.

## 3 II. DISCUSSION

4 Mr. Michaud raises two<sup>1</sup> primary Fourth Amendment issues: whether deploying the NIT  
5 from the Eastern District of Virginia, to Mr. Michaud's computer, located outside that district,  
6 exceeded the scope of the NIT Warrant's authorization; and whether the NIT Warrant lacks  
7 particularity and amounts to a general warrant. In addition to those constitutional issues, Mr.  
8 Michaud raises the issue of a statutory violation, that is, whether the NIT Warrant violates Fed.  
9 R. Crim. P. Rule 41(b). Based on those issues, Mr. Michaud requests suppression of evidence  
10 secured through the NIT and all fruits of that search.

11 a. Whether deploying the NIT to a computer outside of the Eastern District of Virginia  
12 exceeded the scope of the NIT Warrant's authorization.

13 Mr. Michaud argues that the NIT Warrant authorized deployment of the NIT only to  
14 computers within one geographical location, the Eastern District of Virginia. Dkt. 65, at 15-17.  
15 Dkt. 139, at 3, 4. He asserts that because the FBI deployed the NIT to Mr. Michaud's computer,  
16 located outside of that district, the search and seizure exceeded the scope of the NIT Warrant. *Id.*

17 The Fourth Amendment to the United States Constitution provides that "no Warrants  
18 shall issue, but upon probable cause, supported by Oath or affirmation, and particularly  
19 describing the place to be searched, and the persons or things to be seized." If the execution of a  
20 search or seizure exceeds the scope of a warrant, the subsequent search or seizure is

---

21 <sup>1</sup> In his motion for a *Franks* hearing, Mr. Michaud raised a third constitutional issue,  
22 challenging the probable cause underlying the NIT Warrant, which the Court denied at oral  
23 argument. Dkt. 135. *See* Dkt. 65, at 5-15. However, even if the NIT Warrant was not supported  
24 by probable cause, as Mr. Michaud argued, reliance on the NIT Warrant was objectively  
reasonable, *see supra*, so suppression is not warranted. *U.S. v. Needham*, 718 F.3d 1190, 1194  
(9<sup>th</sup> Cir. 2013).



1 unconstitutional. *Horton v. California*, 496 U.S. 128, 140 (1990). Whether a search or seizure  
2 exceeds the scope of a warrant is an issue that is determined “through an objective assessment of  
3 the circumstances surrounding the issuance of the warrant, the contents of the search warrant,  
4 and the circumstances of the search.” *U.S. v. Hurd*, 499 F.3d 963, 966 (9th Cir 2007)(*internal*  
5 *quotations and citations omitted*).

6 Mr. Michaud’s argument requires an overly narrow reading of the NIT Warrant that  
7 ignores the sum total of its content. While the NIT Warrant cover sheet does explicitly reference  
8 the Eastern District of Virginia, that reference should be viewed within context:

9 “An application by a federal law enforcement officer . . . requests the  
10 search of the following person or property located in the Eastern District  
11 of Virginia (*identify the person or describe the property to be searched*  
*and give its location*):  
See Attachment A[.]” Dkt. 47-1, at 39.

12 The warrant explicitly invites the magistrate judge to “give its location” in the blank space  
13 provided, wherein the phrase, “See Attachment A,” is inserted. Attachment A, subtitled “Place to  
14 be Searched,” authorizes deployment of the NIT to “all activating computers,” defined as “those  
15 of any user or administrator who logs into [Website A] by entering a username and password.”  
16 *Id.* Attachment A refers to the Eastern District of Virginia as the location of the government-  
17 controlled computer server from which the NIT is deployed. *Id.* A reasonable reading of the NIT  
18 Warrant’s scope gave the FBI authority to deploy the NIT from a government-controlled  
19 computer in the Eastern District of Virginia against anyone logging onto Website A, with any  
20 information gathered by the NIT to be returned to the government-controlled computer in the  
21 Eastern District of Virginia.

22 The warrant application reinforces this interpretation, which is objectively reasonable.  
23 The warrant application, when detailing how the NIT works, explains that the NIT “may cause  
24

1 an activating computer—*wherever located*—to send to a computer controlled by or known to the  
2 government [in the Eastern District of Virginia], network level messages *containing information*  
3 *that may assist in identifying* the computer, *its location*, and other information[.]” Dkt. 47-1, at  
4 ¶46 (emphasis added). The execution of the NIT Warrant is also consistent with and supports this  
5 interpretation. *See* Dkt. 47-5, at ¶¶13-18. Because this interpretation is objectively reasonable,  
6 execution of the NIT Warrant consistent with this interpretation should be upheld, even if there  
7 are other possible reasonable interpretations. *Bergquist v. County of Cochise*, 806 F.2d 1364 (9th  
8 Cir. 1986) (*abrogated on other grounds by City of Canton, Ohio v. Harris*, 489 U.S. 378 (1989)).

9 b. Whether the NIT Warrant lacks specificity and amounts to a general warrant.

10 Mr. Michaud argues in the alternative that if the NIT Warrant did not limit the NIT’s  
11 deployment to computers within one geographic location, the Eastern District of Virginia, the  
12 NIT Warrant is also unconstitutional because it lacks specificity and amounts to a general  
13 warrant. Dkt. 65, at 17; Dkt. 111, at 20.

14 Whether a warrant lacks specificity depends on two factors, particularity and breadth.  
15 “Particularity means the ‘warrant must make clear . . . exactly what it is that he or she is  
16 authorized to search for and seize.’” *United States v. SDI Future Health, Inc.*, 568 F.3d 684, 702  
17 (9<sup>th</sup> Cir. 2009)(quoting *In re Grand Jury Subpoenas Dated Dec. 10, 1987*, 926 F.2d 847, 857 (9<sup>th</sup>  
18 Cir. 1991). Warrants do not lack particularity where they “describe generic categories of items . .  
19 . if a more precise description of the items . . . is not possible.” *Id.* (citing to *United States v.*  
20 *Spilotro*, 800 F.2d 959, 963 (9<sup>th</sup> Cir. 1986)). “Breadth” inquires as to whether the scope of the  
21 warrant exceeds the probable cause on which the warrant is based. *Id.*

22 As a threshold matter, it appears that even if Mr. Michaud was correct in arguing that the  
23 NIT Warrant is unconstitutional because it is a general warrant, suppression may not be required  
24

1 because the officers acted in good faith when executing the warrant. *See supra*, II(c)(3). *See also*,  
2 *United States v. Negrete Gonzales*, 966 F.2d 1277, 1283 (9<sup>th</sup> Cir. 1992) (citing to *United States v.*  
3 *Leon*, 468 U.S. 897 (1984)). The NIT Warrant does not, however, lack sufficient specificity. The  
4 warrant states with particularity exactly what is to be searched, namely, computers accessing  
5 Website A. Dkt. 47-1, at 37. According to the warrant application upon which the NIT Warrant  
6 was issued, Website A is unmistakably dedicated to child pornography. Although the FBI may  
7 have anticipated tens of thousands of potential suspects as a result of deploying the NIT, that  
8 does not negate particularity, because it would be highly unlikely that Website A would be  
9 stumbled upon accidentally, given the nature of the Tor network.

10 The second factor, breadth, considers whether the NIT Warrant exceeded the probable  
11 cause on which it was issued. While the warrant application certainly provides background facts  
12 not found in the NIT Warrant itself, *compare* Dkt. 47-1, at 2-36 and Dkt. 47-1, at 37-40, the NIT  
13 Warrant does not authorize anything beyond what was requested by the warrant application. In  
14 fact, the NIT Warrant language found in Attachment A and Attachment B is identical to the  
15 scope of the warrant requested. *Id.*, at 4, 5, 37, 38. Both the particularity and breadth of the NIT  
16 Warrant support the conclusion that the NIT Warrant did not lack specificity and was not a  
17 general warrant.

18 c. Whether the NIT Warrant violates Fed. R. Crim. P. Rule 41(b).

19 Concerning Fed. R. Crim. P. Rule 41(b), Mr. Michaud makes three primary arguments:  
20 (1) the NIT Warrant violates the plain text of Rule 41(b), (2) the Rule 41(b) violation requires  
21 suppression, because the violation was the result of an intentional and deliberate disregard of  
22 Rule 41(b), and results in prejudice to Mr. Michaud, and (3) the good faith exception does not  
23 “save” the Rule 41(b) violation because it does not apply. Dkt. 26, at 8-16; Dkt. 69, at 3-11.  
24

1           ***1. Plain text of Rule 41(b).***

2           According to Mr. Michaud, the NIT Warrant violates the general provision of Rule 41(b),  
3 subdivision (b)(1), because the rule prohibits the magistrate judge in the Eastern District of  
4 Virginia from issuing a warrant to search or seize a computer outside of her district, including  
5 Vancouver, Washington. Dkt. 26, at 11-13. Mr. Michaud also argues against the applicability of  
6 the rule's other subdivisions, which carve out exceptions for searches outside of the district. Dkt.  
7 26, at 13, 14.

8           18 U.S.C. § 3103, which governs the grounds for issuing search warrants, directly  
9 incorporates Rule 41(b). Subdivision (b)(1) states the general rule, that “a magistrate with  
10 authority in the district . . . has the authority to issue a warrant to search for and seize a person or  
11 property located within the district.” Fed. R. Crim. P. 41(b)(1). Exceptions apply where a person  
12 or property “might move or be moved outside the district before the warrant is executed,”  
13 subdivision (b)(2), when federal law enforcement investigates terrorism, subdivision (b)(3),  
14 when a tracking device installed within the district travels outside the district, subdivision (b)(4),  
15 and where the criminal activities occur on a United States territory, commonwealth, or other  
16 location under the control of the United States other than a state, subdivision (b)(5).

17           Rule 41(b) is to be applied flexibly, not rigidly. *United States v. Koyomejian*, 970 F.2d  
18 536, 542 (9<sup>th</sup> Cir. 1992). In *United States v. New York Tel. Co.*, 434 U.S. 159 (1977), the  
19 Supreme Court addressed the general relationship of technology and Rule 41, concluding that  
20 Rule 41 “is sufficiently flexible to include within its scope electronic intrusions authorized upon  
21 a finding of probable cause.” *Id.*, at 169. The *New York Tel. Co.* court noted that a flexible  
22 reading of Rule 41 is reinforced by Fed. R. Crim. P. 57(b), which provides that in the absence of  
23 controlling law, “a judge may regulate practice in any manner consistent with federal law, these  
24

1 rules and the local rules[.]” *Id.*, at 170.<sup>2</sup> Although *New York Tel. Co.* addressed a now-  
2 superseded subdivision of Rule 41 and a different technology, the pen register, the flexibility  
3 applied to Rule 41 has since been applied to subsection (b) of Rule 41. *See, e.g., Koyomejian*,  
4 970 F.2d at 542.

5 In this case, even applying flexibility to Rule 41(b), the Court concludes that the NIT  
6 Warrant technically violates the letter, but not the spirit, of Rule 41(b). The rule does not directly  
7 address the kind of situation that the NIT Warrant was authorized to investigate, namely, where  
8 criminal suspects geographical whereabouts are unknown, perhaps by design, but the criminal  
9 suspects had made contact via technology with the FBI in a known location. In this context, and  
10 when considering subdivision (b)(1), a cogent, but ultimately unpersuasive argument can be  
11 made that the crimes were committed “within” the location of Website A, Eastern District of  
12 Virginia, rather than on personal computers located in other places under circumstances where  
13 users may have deliberately concealed their locations. However, because the object of the search  
14 and seizure was Mr. Michaud’s computer, not located in the Eastern District of Virginia, this  
15 argument fails. In a similar vein, a reasonable, but unconvincing argument can be made that  
16 subdivision (b)(2) applies, given the interconnected nature of communications between Website  
17 A and those who accessed it, but because Mr. Michaud’s computer was not ever physically  
18 within the Eastern District of Virginia, this argument also fails.

---

19  
20  
21 <sup>2</sup> Although not argued by the parties, a flexible interpretation of Rule 41(b) that accounts  
22 for changes in technology may also reconcile Rule 41(b) with 18 U.S.C. § 3103a, which provides  
23 that “[I]n addition to the grounds for issuing a warrant [under Rule 41(b)], a warrant may be  
24 issued . . . for . . . any property that constitutes evidence of a criminal offense.” As the parties  
appeared to agree at oral argument, § 3103a was enacted to codify the elimination of the mere  
evidence rule overturned in *Warden v. Hayden*, 387 U.S. 294 (1967), but neither party offered a  
satisfactory explanation to reconcile § 3103a with § 3103 and Rule 41(b).

1 Finally, applying subdivision (b)(4), which allows for tracking devices installed within  
2 one district to travel to another, stretches the rule too far. If the “installation” occurred on the  
3 government-controlled computer, located in the Eastern District of Virginia, applying the  
4 tracking device exception breaks down, because Mr. Michaud never controlled the government-  
5 controlled computer, unlike a car with a tracking device leaving a particular district. If the  
6 installation occurred on Mr. Michaud’s computer, applying the tracking device exception again  
7 fails, because Mr. Michaud’s computer was never physically located within the Eastern District  
8 of Virginia. The Court must conclude that the NIT Warrant did technically violate Rule 41(b),  
9 although the arguments to the contrary are not unreasonable and do not strain credulity.

10 **2. *Prejudice to Mr. Michaud and intentional and deliberate disregard of Rule 41(b).***

11 Rule 41(b) violations are categorized as either fundamental, when of constitutional  
12 magnitude, or technical, when not of constitutional magnitude. *Negrete-Gonzales*, 966 F.2d at  
13 1283. As concluded above, the NIT Warrant did not fail for constitutional reasons, but rather  
14 was the product of a technical violation of Rule 41(b). Sec. II(c)(1). In cases where a technical  
15 Rule 41(b) violation occurs, courts may suppress where a defendant suffers prejudice, “in the  
16 sense that the search would not have occurred . . . if the rule had been followed,” or where law  
17 enforcement intentionally and deliberately disregarded the rule. *United States v. Weiland*, 420  
18 F.3d 1062, 1071 (9<sup>th</sup> Cir. 2005) (citing to *United States v. Martinez-Garcia*, 397 F.3d 1205, 1213  
19 (9<sup>th</sup> Cir. 2005)).

20 In this case, suppression is not warranted on the basis of the technical violation of Rule  
21 41(b), because the record does not show that Mr. Michaud was prejudiced or that the FBI acted  
22 intentionally and with deliberate disregard of Rule 41(b). First, considering the prejudice, Mr.  
23 Michaud would have the Court interpret the definition of prejudice found in *Weiland* and  
24

1 elsewhere, “in the sense that the search would not have occurred . . . if the rule had been  
2 followed,” to mean that defendants suffer prejudice whenever a search occurs that violates Rule  
3 41(b). This interpretation makes no sense, because under that interpretation, all searches  
4 executed on the basis of warrants in violation of Rule 41(b) would result in prejudice, no matter  
5 how small or technical the error might be. Such an interpretation would defeat the need to  
6 analyze prejudice separately from the Rule 41(b) violation. Tracing the origin of the definition  
7 used in *Weiland* to its early use in the Ninth Circuit yields a more sensible interpretation of the  
8 well-established definition: “in the sense that the search would not have occurred . . . if the rule  
9 had been followed” suggests that courts should consider whether the evidence obtained from a  
10 warrant that violates Rule 41(b) could have been available by other lawful means, and if so, the  
11 defendant did not suffer prejudice. *See United States v. Vasser*, 648 F.2d 507, 511 (9th Cir.  
12 1980).

13 Applying that interpretation here, Mr. Michaud did not suffer prejudice. Mr. Michaud has  
14 no reasonable expectation of privacy of the most significant information gathered by deployment  
15 of the NIT, Mr. Michaud’s assigned IP address, which ultimately led to Mr. Michaud’s  
16 geographic location. *See United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008). Although  
17 the IP addresses of users utilizing the Tor network may not be known to websites, like Website  
18 A, using the Tor network does not strip users of all anonymity, because users accessing Website  
19 A must still send and receive information, including IP addresses, through another computer,  
20 such as an Internet Service Provider, at a specific physical location. Even though difficult for the  
21 Government to secure that information tying the IP address to Mr. Michaud, the IP address was  
22 public information, like an unlisted telephone number, and eventually could have been  
23 discovered.

1 Mr. Michaud also fails to show that the FBI acted intentionally and with deliberate  
2 disregard of Rule 41(b). Mr. Michaud's arguments to the contrary rely only on thin inferences,  
3 which are insufficient. Mr. Michaud argues that the Rule 41(b) violation of the NIT Warrant,  
4 which was predicated on the FBI's warrant application, was so obvious that the mere submission  
5 of the warrant application shows an intent to disregard the rule. The NIT Warrant did technically  
6 violate Rule 41(b), but reasonable, although unavailing arguments can be made to the contrary.  
7 *See infra*, II(a) and (c)(2). Mr. Michaud points to one opinion by a magistrate judge, who denied  
8 a similar warrant application seeking authorization to search "Nebraska and elsewhere," as  
9 evidence of intent and deliberate disregard, but that magistrate judge, who sits in one of ninety-  
10 four judicial districts, ruled on an unsettled area of the law where there is no controlling circuit or  
11 Supreme Court precedent. *See United States v. Cottom* Findings and Recommendations,  
12 Nebraska CR13-0108JFB. *See also*, Dkt. 69-1; Dkt. 111-2. Mr. Michaud also argues intent and  
13 deliberate disregard are shown by that the fact that the Government has elsewhere argued that  
14 Rule 41(b) should be amended to account for changes in technology, but this argument also fails,  
15 given that reasonable minds can differ as to the degree of Rule 41(b)'s flexibility in uncharted  
16 territory. *See also*, Fed. R. Crim. P. 57(b).<sup>3</sup>

17 **3. Good faith.**

18 Mr. Michaud also argues that, because the NIT Warrant violated Rule 41(b) and the  
19 Constitution, suppression is required because the good faith exception does not apply; and that  
20 the FBI did not execute the NIT Warrant in good faith.

---

21  
22  
23 <sup>3</sup> It appears clear that Fed. R. Crim. P. 41 or 18 U.S.C. § 3103 should be modified to  
24 provide for issuance of warrants that involve modern technology. Furthermore, said rule only  
applies to magistrate judges and state judges, and does not address limits on warrants issued by  
other federal judicial officers.



1 Where a warrant is executed in good faith, even if the warrant itself is subsequently  
2 invalidated, evidence obtained need not be suppressed. *United States v. Leon*, 468 U.S. 897, 922  
3 (1984). Warrants may be invalidated for technical or fundamental (constitutional) violations. *See*  
4 *id.*, at 918 (technical violation) and *Negrete-Gonzales*, 966 F.2d at 1283 (constitutional  
5 violation). Whether a warrant is executed in good faith depends on whether reliance on the  
6 warrant was objectively reasonable. *Id.*, at 922.

7 ““Searches pursuant to a warrant will rarely require any deep inquiry into  
8 reasonableness.”” *Leon*, at 922 (quoting *Illinois v. Gates*, 462 U.S., 213, 267 (1983)).  
9 Nonetheless, reliance on the NIT Warrant was objectively reasonable. *See infra*, II(a) and (c)(2).  
10 Mr. Michaud’s argument that the good faith exception does not apply, because *Weiland*  
11 overrules *Negrete-Gonzales*, which explicitly analyzed good faith in the context of a Rule 41(b)  
12 violation, is unavailing. Although the *Weiland* court makes no mention of good faith, it did not  
13 reach the issue, because it affirmed a lower court’s finding that suppression was not appropriate  
14 where there was no showing of a Rule 41(b) violation of constitutional magnitude, prejudice to  
15 the defendant, or intentional and deliberate disregard of the rule. *Id.*, at 1072. Because reliance  
16 on the NIT Warrant was objectively reasonable, the officers executing the warrant acted in good  
17 faith, and suppression is unwarranted.

### 18 III. CONCLUSION

19 “The Fourth Amendment incorporates a great many specific protections against  
20 unreasonable searches and seizures. The contours of these protections in the context of  
21 computer searches pose difficult questions.” *United States v. Adjani*, 452 F.3d 1140, 1152  
22 (9th Cir. 2006)(*internal quotations and citations omitted*). What was done here was  
23 ultimately reasonable. The NIT Warrant was supported by probable cause and  
24

1 particularly described the places to be searched and the things to be seized. Although the  
2 NIT Warrant violated Rule 41(b), the violation was technical in nature and does not  
3 warrant suppression. Mr. Michaud suffered no prejudice, and there is no evidence that  
4 NIT Warrant was executed with intentional and deliberate disregard of Rule 41(b).  
5 Instead, the evidence shows that the NIT Warrant was executed in good faith. Mr.  
6 Michaud's motions to suppress should be denied.

7 \* \* \*

8 THEREFORE, it is HEREBY ORDERED that Defendant's Motion to Suppress Evidence  
9 (Dkt. 26) is DENIED. Defendant's Second Motion to Suppress Evidence and Motion for *Franks*  
10 Hearing (Dkt. 65) is DENIED.

11 The Clerk is directed to send uncertified copies of this Order to all counsel of record and  
12 to any party appearing *pro se* at said party's last known address.

13 Dated this 28<sup>th</sup> day of January, 2016.

14 

15 ROBERT J. BRYAN  
16 United States District Judge

1  
2  
3  
4  
5  
6 UNITED STATES DISTRICT COURT  
7 WESTERN DISTRICT OF WASHINGTON  
8 AT TACOMA

9 UNITED STATES OF AMERICA,

CASE NO. 3:15-cr-05351RJB

10 Plaintiff,

v.

ORDER DENYING DISMISSAL  
AND EXCLUDING EVIDENCE

11 JAY MICHAUD,

12 Defendant.

13  
14 This matter came before the court on the defendant's Motion to Dismiss the Indictment  
15 (Dkt. 178). In supporting briefing, the defendant also suggested an alternative remedy by  
16 excluding evidence (Dkt. 210). The court is familiar with the records and files herein and heard  
17 oral argument on the motion on May 25, 2016.


18 For the reasons stated orally on the record, evidence of the N.I.T., the search warrant  
19 issued based on the N.I.T., and the fruits of that warrant should be excluded and should not be  
20 offered in evidence at trial. The court should not now order dismissal.

21 The Motion to Dismiss (Dkt. 178) should be DENIED IN PART and GRANTED IN  
22 PART to the foregoing extent.

23 IT IS SO ORDERED.  
24

1 The Clerk is directed to send uncertified copies of this Order to all counsel of record and  
2 to any party appearing *pro se* at said party's last known address.

3 Dated this 25<sup>th</sup> day of May, 2016.

4 

5  
6 ROBERT J. BRYAN  
United States District Judge

7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA,

v.

GABRIEL WERDENE,

*Defendant.*

CRIMINAL ACTION  
NO. 15-434

PAPPERT, J.

MAY 18, 2016

**MEMORANDUM**

Gabriel Werdene (“Werdene”) was indicted on September 17, 2015 on one count of possessing and attempting to possess child pornography pursuant to 18 U.S.C. §§ 2252(a)(4)(B) and (b)(2). The indictment was based on evidence obtained during a June 17, 2015 search of Werdene’s Bensalem, Pennsylvania home, which was conducted in accordance with a warrant issued by a magistrate judge in this judicial district. The Federal Bureau of Investigation (“FBI”) identified Werdene after a magistrate judge in Virginia issued a warrant permitting agents to deploy software that revealed the IP addresses of visitors to a child pornography website called Playpen.<sup>1</sup> FBI agents matched Werdene’s Playpen username, “thepervert,” to his IP address and then located his home in Bensalem based on that information.

Playpen’s patrons accessed the website through software called “Tor,” an acronym for “The onion router.” Tor conceals the IP addresses of people who visit certain websites, in Werdene’s case a website purveying child pornography. Otherwise stated, Tor enables people to use websites like Playpen to view, upload and share child pornography without being identified by traditional law enforcement investigative methods. To circumvent Tor, the FBI used a

---

<sup>1</sup> The parties refer to Playpen as “Website A,” ostensibly to preserve the anonymity of the site during the continued investigation of its users and administrators. A number of published articles and judicial opinions, *see infra* Section I.E, have already identified “Website A” as Playpen, eliminating the need for any further efforts to conceal its identity.

Network Investigative Technique (“NIT”). The NIT caused software to be activated whenever a Playpen user logged into the website with his username and password. The software caused the Playpen user’s computer to reveal its IP address to the FBI. The search warrant issued by the Virginia magistrate authorized the NIT.

Werdene moves to suppress the evidence seized from his home, arguing primarily that the magistrate judge in Virginia lacked jurisdiction under Federal Rule of Criminal Procedure 41 to authorize the NIT. Werdene contends that this violation of a procedural rule warrants suppression. While Rule 41 did not authorize the issuance of the warrant in Virginia, suppression is not the appropriate remedy. The magistrate judge’s failure to comply with Rule 41 did not violate Werdene’s Fourth Amendment rights because Werdene had no expectation of privacy in his IP address, and certainly not one that society would recognize as reasonable. Even if Werdene’s constitutional rights were violated, the good faith exception to the exclusionary rule precludes suppression. Finally, any nonconstitutional violation of Rule 41 did not prejudice Werdene, as that term has been defined by the Third Circuit Court of Appeals in the Rule 41 context. The Court denies the motion.

## I.

Playpen operated on the “dark web,” a collection of websites that use anonymity tools to hide those websites’ IP addresses and mask the identity of their administrators. Websites on the dark web can only be accessed using certain software such as Tor. (*See* Gov’t. Mem. in Opp. to Def.’s Mot. to Suppress (“Gov’t’s Opp.”), Ex. 1 ¶¶ 7–10, ECF No. 21.) Playpen, as its name connotes in this context, was “dedicated to the advertisement and distribution of child pornography, [and] the discussion of matters pertinent to child sexual abuse.” (*Id.*, Ex. 1 ¶ 6.) The website’s home page displayed an image of two partially clothed prepubescent females with

their legs spread. (*Id.*, Ex. 1 ¶ 12.) Upon arriving at the home page, a user was prompted to either register an account or login using his pre-existing username and password. (*Id.*) Prior to registering an account, a message was displayed which told the user, among other things, “NOT [to] . . . enter a real [email] address” and “[f]or your security you should not post information here that can be used to identify you.” (*Id.*, Ex. 1 ¶ 13.) The message also stated that “[t]his website is not able to see your IP address and can not [sic] collect or send any other form of information to your computer except what you expressly upload.” (*Id.*)

After successfully registering and logging into the site, the user reached a page which listed a number of “forums” or discussion boards on which users could post images, videos or text regarding various topics. The “forums” included “Jailbait – Boy,” “Jailbait – Girl,” “Preteen – Boy,” “Preteen – Girl,” “Jailbait Videos,” “Jailbait Photos,” “Pre-teen Videos,” “Pre-Teen Photos,” “Family – Incest” and “Toddlers.” (*Id.*, Ex. 1 ¶ 14.) Within the pre-teen videos and photos forums were “subforums” titled “Girls [hardcore],” “Boys [hardcore],” “Girls [softcore/non-nude]” and “Boys [softcore/non-nude].”<sup>2</sup> (*Id.*) Each forum contained a topic with titles, an author and the number of replies and views. (*Id.*, Ex. 1 ¶ 16.) Upon accessing a topic, the original post appeared at the top of the page with all corresponding replies to the original post below. (*Id.*) Typical posts contained text, links to external sites, and/or images. (*Id.*)

Playpen also included features available to all users of the website referred to as “Playpen Image Hosting” and “Playpen Video Hosting.” (*Id.*, Ex. 1 ¶ 23.) Those pages allowed users to upload images and videos of child pornography for other users to view. (*Id.*) Over 1,500 unique users visited Playpen daily and over 11,000 unique users visited the site over the course of a

---

<sup>2</sup> FBI Special Agent Douglas Macfarlane (“Agent Macfarlane”) stated in his warrant application to employ the NIT that “jailbait refers to underage but post-pubescent minors.” (Gov’t’s Opp., Ex. 1 ¶ 14 n.4.) Furthermore, “hardcore” typically depicts “penetrative sexually explicit conduct,” “softcore” depicts “non-penetrative sexually explicit conduct,” and “non-nude” depicts “subjects who are fully or partially clothed.” (*Id.*, Ex. 1 ¶ 14 n.5.)

week. (*Id.*, Ex. 1 ¶ 19.) According to statistics on the website, by March 2015 Playpen contained a total of 117,773 posts, 10,622 total topics and 214,898 total members. (*Id.*, Ex. 2 ¶ 12.)

A.

Playpen operated on and was only accessible through Tor. (*Id.*, Ex. 1 ¶ 7.) Unlike a public website, a user could not reach Playpen through a traditional web search engine, such as Google. (*Id.*, Ex. 1 ¶ 10.) Rather, he could only access the website by using Tor and inputting the “particular . . . combination of letters and numbers that” matched Playpen’s specific Tor-based web address. (*Id.*, Ex. 1 ¶¶ 9–10; Hr’g Tr. 38:9–13, ECF No. 29.)

Although the United States Naval Research Laboratory initially designed and implemented Tor for the primary purpose of protecting government communications, it is now “free software, [ ] available worldwide” to the public. (Gov’t’s Opp., Ex. 1 ¶ 7; Hr’g Tr. 7:13–17.) In order to access the Tor network, a user must take affirmative steps to install the software on his computer by either downloading an add-on to his web browser or downloading the Tor software available on its website. (Gov’t’s Opp., Ex 1 ¶ 7.)

The use of Tor thwarts traditional IP identification and investigative techniques. (*Id.*, Ex. 2 ¶ 23.) Under those traditional methods, FBI agents can review IP address logs after they seize a website to determine which IP addresses visited the site. (*Id.*, Ex. 1 ¶ 22.) They can then conduct a publicly available search to determine which internet service providers (“ISPs”) owned the target IP address and issue a subpoena to the ISP to ascertain the identity of the user. (*Id.*)

The Tor software masks a user’s IP address by “bouncing their communications around a distributed network of relay computers run by volunteers all around the world.” (*Id.*, Ex. 1 ¶ 8.) As a result, “traditional IP identification techniques are not viable” because the last computer or



“exit node” is not the IP address of the actual user who visits the website. (*Id.*; *id.*, Ex. 2 ¶ 23.) It is also impossible to trace the IP address back to the originating computer. (*Id.*, Ex. 2 ¶ 23.) The Tor network “operates similarly to a proxy server—that is, a computer through which communications are routed to obscure a user’s true location.” (*Id.*, Ex. 1 ¶ 8.)

Tor also allows websites, such as Playpen, to operate as a “hidden service.” (*Id.*, Ex. 1 ¶ 9.) Tor masks the website server’s IP address and replaces it with a Tor-based web address. (*Id.*) The Tor-based address is usually a series of algorithm-generated characters such as “asdlk8fs9dfku7f” followed by the suffix “.onion.” (*Id.*) The user may obtain Playpen’s specific address from other users or through a link posted on one of Tor’s “hidden services” pages dedicated to child pornography and pedophilia. (*Id.*, Ex. 1 ¶ 10.)

## **B.**

In December 2014, a foreign law enforcement agency informed the FBI that it suspected a United States-based IP address was associated with Playpen. (*Id.*, Ex. 1 ¶ 28.) The FBI confirmed through a publicly available search that the IP address was owned by Centrilogic, a server hosting company headquartered in Lenoir, North Carolina. (*Id.*) The FBI subsequently obtained a search warrant for the server. (*Id.*) FBI agents examined the server and determined that it contained a copy of Playpen. They then stored the copy of the website on a computer server at a government facility in Newington, Virginia. Newington is located in the Eastern District of Virginia. (*Id.*)

Additional investigation revealed that a resident of Naples, Florida had administrative control of Playpen and the computer server in Lenoir. (*Id.*) On February 19, 2015 FBI personnel executed a court-authorized search of the suspected administrator’s residence in Naples. (*Id.*, Ex. 1 ¶ 30.) The FBI arrested the suspect and assumed administrative control of Playpen. (*Id.*)

On February 20, 2015, Agent Macfarlane applied to a United States Magistrate Judge in the Eastern District of Virginia for a warrant to use the NIT while the FBI assumed administrative control of Playpen on a copy of its server in Newington. (*See generally id.*, Ex. 1.)

Agent Macfarlane stated in the warrant application that the NIT was necessary to overcome the obstacles presented by Tor’s masking capabilities. (*Id.*, Ex. 1 ¶ 31.) He stated that “other investigative procedures that are usually employed in criminal investigations of this type have been tried and failed or reasonably appear to be unlikely to succeed if they are tried.” (*Id.*) The agent represented that the search would aid the FBI in its investigation by revealing “information that may assist in identifying the user’s computer, its location, and the user of the computer.” (*Id.*, Ex. 1 ¶ 34.) He explained in the warrant application that the NIT would “augment” the normal content that websites send to its visitors with “additional computer instructions.” (*Id.*, Ex. 1 ¶ 33.) Specifically, those instructions “are designed to cause the user’s ‘activating’ computer to transmit certain information to a computer controlled by or known to the government,” including the “activating” computer’s actual IP address.<sup>3</sup> (*Id.*, Ex. 1 ¶ 33, Attach. B.) The NIT would deploy “each time that any user or administrator log[ged] into Playpen by entering a username and password.” (*Id.*, Ex. 1 ¶ 36.) The FBI could then link a username and its corresponding activity on the site with an IP address. (*Id.*, Ex. 1 ¶ 37.)

Agent Macfarlane explained that the “NIT may cause an activating computer—*wherever located*—to send to a computer controlled by or known to the government network level messages containing information that may assist in identifying the computer, its location, other information about the computer and the user of the computer.” (*Id.*, Ex. 1 ¶ 46 (emphasis

---

<sup>3</sup> Other information gathered from the NIT included: (1) a unique identifier generated by the NIT to distinguish data from that particular computer; (2) the type of operating system running on the computer; (3) information about whether the NIT has already been delivered to the “activating” computer; (4) the “activating” computer’s host name; (5) the “activating” computer’s active operating system username; and (6) the “activating” computer’s media access control (“MAC”) address. (Gov’t’s Opp., Ex. 1 Attach. B.)

added).) In Attachment A to the warrant application, which identified the “place to be searched,” Agent Macfarlane stated that the NIT would be “deployed on the computer server. . . . located at a government facility in the Eastern District of Virginia.” (*Id.*, Ex. 1 Attach. A.) It stated that the NIT would seek information from the “activating computers,” which “are those of any user or administrator who logs into [Playpen] by entering a username and password.” (*Id.*) On February 20, 2015, the magistrate judge issued the search warrant. (*Id.*, Ex. 1.)

### C.

While monitoring activity on Playpen after seizing a copy of the server, FBI agents observed someone with the username “thepervert” posting occasionally on the website’s forums. (*Id.*, Ex. 2 ¶¶ 25–27.) The profile page indicated that “thepervert” created his profile on January 26, 2015 and had been actively logged into the website for 10 hours and 18 minutes between that date and March 1, 2015. (*Id.*, Ex. 2 ¶ 26.) During that time, “thepervert” made approximately six postings on Playpen which included, among other things, hyperlinks to forums on both Playpen and external websites containing child pornography. (*Id.*, Ex. 2 ¶ 27.)

On February 28, 2015, after the NIT had already been deployed, “thepervert” logged into Playpen by entering his username and password. (*Id.*, Ex. 2 ¶ 28.) That triggered certain information on his computer, including his IP address, to be transmitted to the government. (*Id.*) During that browsing session, “thepervert” accessed forums depicting child pornography. (*Id.*, Ex. 2 ¶ 29.)

Using publicly available websites, FBI agents were able to determine that Comcast Cable (“Comcast”) operated the suspect’s IP address. (*Id.*, Ex. 2 ¶ 30.) They served upon Comcast an administrative subpoena/summons requesting information related to the IP address associated

with “thepervert.” (*Id.*, Ex. 2 ¶ 31.) According to the information received from Comcast, the IP address was assigned to Werdene. (*Id.*, Ex. 2 ¶¶ 31–33.)

On June 17, 2015, FBI agents sought and obtained from a Magistrate Judge in the United States District Court for the Eastern District of Pennsylvania a warrant to search Werdene’s home in Bensalem for “evidence, contraband, [and] fruits/instrumentalities” of child pornography. (*Id.*) On that same day, FBI agents searched Werdene’s home and obtained a laptop, a USB drive contained in a safe and one DVD, all containing child pornography. (Gov’t’s Opp. at 8.) Werdene lived alone and was not home at the time of the search. (*Id.*) FBI agents later interviewed him, where he admitted to using and downloading the material on his laptop. (*Id.*) Werdene was indicted on September 17, 2015. (*Id.*)

**D.**

On February 11, 2016 Werdene filed a motion to suppress all physical evidence seized from his home and “all fruits therefrom,” including any inculpatory statements he made. (Def.’s Mot. to Suppress at \*1, ECF No. 19.) He argues that the government “knowingly circumvented” Federal Rule of Criminal Procedure 41, which “limits the authority of a magistrate judge to issue a warrant and “serves as a bulwark against the very type of sweeping dragnet searches and unrestrained government surveillance that occurred in this case.” (Def.’s Mem. in Supp. of Mot. to Suppress (“Def.’s Mem.”) at 9, ECF No. 19.) He argues that the violation of Rule 41 is “of constitutional magnitude” and the evidence seized pursuant to the NIT should be suppressed. (*Id.* at 15–16.) He further argues that even if the Court does not find a constitutional violation, suppression is warranted because he was prejudiced by the government’s violation of the Rule. (*Id.* at 16–17.) Werdene also contends that the FBI acted with intentional and deliberate

disregard of Rule 41 because they misled the magistrate judge “with respect to the true location of the activating computers to be searched.” (*Id.* at 17.)

The Government argues that “[t]he fact that Rule 41 does not explicitly authorize some procedure does not mean that those procedures are unlawful.” (Gov’t’s Opp. at 17.) It argues that under these circumstances, Werdene’s use of Tor made it impossible for FBI agents to comply with the requirements of Rule 41 because he “made sure that his location could not be found.” (*Id.* at 18.) The Government further states that even if there was a violation of Rule 41, suppression is not the appropriate remedy because it was not of constitutional magnitude and there is no evidence that the FBI agents engaged in any conduct warranting application of the exclusionary rule. (*Id.* at 20–26.) The Court held a hearing on the motion on April 7, 2016. (ECF No. 27.)

#### E.

A number of federal courts have recently issued opinions in cases arising from the same NIT application and warrant issued in this case. *See United States v. Levin*, 15-cr-10271, 2016 WL 2596010 (D. Mass. May 5, 2016); *United States v. Arterbury*, 15-cr-182 (N.D. Okla. Apr. 25, 2016) (report and recommendation); *United States v. Epich*, 15-cr-163, 2016 WL 953269 (E.D. Wis. Mar. 14, 2016); *United States v. Stamper*, No. 15-cr-109 (S.D. Ohio Feb. 19, 2016); *United States v. Michaud*, 15-cr-05351, 2016 WL 337263 (W.D. Wash. Jan. 28, 2016). Similar to Werdene, the defendants in those cases lived outside of the Eastern District of Virginia and sought to suppress the evidence against them because of the Government’s alleged violations of Rule 41.<sup>4</sup>

---

<sup>4</sup> The issue that the court addressed in *Stamper* was not suppression for violation of Rule 41, but instead suppression for violation of the Fourth Amendment.

Although the courts generally agree that the magistrate judge in Virginia lacked authority under Rule 41 to issue the warrant, they do not all agree that suppression is required or even appropriate. *Compare Michaud*, 2016 WL 337263, at \*6–7 (finding violation of Rule 41(b) but suppression unwarranted because defendant was not prejudiced and FBI agents acted in good faith), *and Epich*, 2016 WL 953269, at \*2 (rejecting Defendant’s contention that Rule 41 was violated and finding suppression unwarranted even if it was), *with Levin*, 2016 WL 2596010, at \*7–15 (finding suppression warranted because Rule 41 “implicates substantive judicial authority,” Defendant was prejudiced even if the violation was technical, and the good faith exception to the exclusionary rule is not available because the warrant was void *ab initio*), *and Arterbury*, slip op. at 13–29 (same).

## II.

Rule 41(b) describes five scenarios in which a magistrate judge has authority to issue a warrant. Subsection (b)(1) states the general rule that “a magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property located within the district.” FED. R. CRIM. P. 41(b)(1). The following four subsections provide that that a magistrate judge has authority to issue a warrant: (2) “if the person or property is located within the district but might move or be moved outside the district before the warrant is executed;” (3) if the magistrate judge sits in a district in which activities related to terrorism have occurred; (4) to install a tracking device within the district, though the magistrate judge may authorize the continued use of the device if the person or object subsequently moves or is moved outside of the district; and (5) where the criminal activities occur in the District of Columbia, any United States territory, or on any land or within any building outside of the country owned by the United States or used by a United States diplomat. FED. R. CRIM. P. 41(b)(2)–(5).

Werdene argues that the NIT warrant “is not authorized under any of these sections, and, therefore, plainly unlawful.” (Def.’s Mem. at 11.) He contends that in this case the “actual ‘place to be searched’ was not the server, but the ‘activating computers’ that would be forced to send data to that server.” (*Id.* at 13.) Accordingly, he contends that since his computer was located in Bensalem, outside the magistrate judge’s jurisdiction in the Eastern District of Virginia, the magistrate judge did not have authority to issue the warrant under any of Rule 41(b)’s five subsections.

During the hearing, Werdene’s counsel introduced as the lone defense exhibit a December 22, 2014 letter from United States Deputy Assistant Attorney General David Bitkower to Judge Reena Raggi, Chair of the Advisory Committee on Criminal Rules, regarding “Response to Comments Concerning Proposed Amendment to Rule 41.”<sup>5</sup> (Def.’s Ex. 1.) The letter addresses various issues related to proposed amendments to Rule 41, including concerns regarding the Fourth Amendment’s particularity and notice requirements, Title III wiretap orders, “remote search techniques” and, relevant to this case, new standards for obtaining a warrant “in cases involving Internet anonymizing technology.” (Def.’s Ex. at 1–2.)

In a section titled “Concealed through technological means,” the letter states that “[u]nder the proposed amendment, a magistrate judge in a district where activities related to a crime may have occurred will have authority to issue a warrant for a remote search if the location of the computer to be searched ‘has been concealed through technological means.’” (*Id.* at 10.) Counsel for Werdene contends the letter is evidence of a Rule 41 violation in her client’s case because “the law has not caught up with technology” and the evidence should be suppressed because “a violation is . . . a violation.” (Hr’g Tr. 17:15, 18:8–9.) The Court need not address whether or not law enforcement has to cease its investigative efforts while the process to amend

---

<sup>5</sup> Judge Raggi sits on the United States Court of Appeals for the Second Circuit.

the Federal Rules of Criminal Procedure plays out. As explained *infra*, a violation of Rule 41 does not end the inquiry. The facts of this case compel the conclusion that suppression is unwarranted.

The Government does not contend that the NIT warrant falls within any specific subsection of Rule 41. (Gov't's Opp. at 15–20.) It instead argues that Rule 41 is flexible, and the failure of Rule 41 to “authorize some procedure does not mean that those procedures are unlawful.” (*Id.* at 17.) The Government highlights the predicament with which the FBI agents were faced: the Defendant’s use of Tor made it impossible for agents to know in which district it should seek a warrant, and they accordingly “sought [the] warrant in the only logical district—the one in which they had the server on which they would install the NIT.” (*Id.* at 16.)

“Rule 41(b) is to be applied flexibly, not rigidly.” *Michaud*, 2016 WL 337263, at \*5 (citing *United States v. Koyomejian*, 970 F.2d 536, 542 (9th Cir. 1992)). Even a flexible application of the Rule, however, is insufficient to allow the Court to read into it powers possessed by the magistrate that are clearly not contemplated and do not fit into any of the five subsections. *See id.* at \*6 (“In this case, even applying flexibility to Rule 41(b), the Court concludes that the NIT Warrant technically violates the letter, but not the spirit, of Rule 41(b).”).

Subsection (b)(1) states that a magistrate judge may issue a warrant “to search for and seize a person or property located within the district.” The Government does not attempt to argue here, as it has done in similar cases in other districts, that the NIT targeted property in the Eastern District of Virginia because the Defendant initiated contact with the server in that location when accessing the website. *See Levin*, 2016 WL 2596010, at \*5 (“[S]ince Levin . . . ‘retrieved the NIT from a server in the Eastern District of Virginia, and the NIT sent [Levin’s] network information back to the server in that district,’ the government argues that the search . . .



can be understood as occurring within the Eastern District of Virginia.”); *Michaud*, 2016 WL 337263, at \*6 (“[A] cogent, but ultimately unpersuasive argument can be made that the crimes were committed ‘within’ the location of Website A, [the] Eastern District of Virginia, rather than on [a] personal computer located in other places under circumstances where users may have deliberately concealed their locations.”). Rather, the Government argues for a flexible application of the Rule because “as is often the case, Congress has not caught up with the changes in technology.” (Hr’g Tr. at 51:1–2.)

That Congress has “not caught up” with technological advances does not change the fact that the target of the NIT in Werdene’s case was located outside of the magistrate judge’s district and beyond her jurisdiction under subsection (b)(1). The property to be seized pursuant to the NIT warrant was not the server located in Newington, Virginia, but the IP address and related material “[f]rom any ‘activating’ computer” that accessed Playpen. (Gov’t’s Opp., Ex. 1 Attach. A.) Since that material was located outside of the Eastern District of Virginia, the magistrate judge did not have authority to issue the warrant under Rule 41(b)(1).

Subsections (b)(2)–(5) are also inapplicable to the NIT warrant: (b)(2) relates to a person or object located within the district at the time the warrant is issued but that the government has reason to believe might move or be moved outside the district; (b)(3) relates to terrorist activity; (b)(4) permits tracking devices to be installed on a person or property within the district; and (b)(5) allows the magistrate judge to issue a warrant when the activity occurs in certain territories outside of the district, none of which are applicable here. Subsections (b)(2) and (b)(4), the only provisions potentially applicable to this case, are both premised on the person or property being located within the district. It is uncontested that the computer information that the NIT targeted

was at all relevant times located beyond the boundaries of the Eastern District of Virginia. The magistrate judge was accordingly without authority to issue the NIT warrant under Rule 41.

### III.

“There are two categories of Rule 41 violations: those involving constitutional violations, and all others.” *United States v. Simons*, 206 F.3d 392, 403 (4th Cir. 2000) (citations omitted) (cited with approval in *United States v. Slaey*, 433 F. Supp. 2d 494, 498 (E.D. Pa. 2006) and *United States v. Sampson*, No. 07-cr-389, 2008 WL 919528, at \*4 (M.D. Pa. Mar. 31, 2008)). Courts have described violations of Rule 41 as either: (1) “substantive” or “constitutional” violations; or (2) “ministerial” or “procedural” violations. *See United States v. Levin*, No. 15-cr-10271, 2016 WL 2596010, at \*7 (D. Mass. May 5, 2016) (distinguishing between “substantive” and “procedural” violations of Rule 41); *see also United States v. Krueger*, 809 F.3d 1109, 1114 (10th Cir. 2015) (finding that the inquiry begins by determining whether the Rule 41 violation was of “constitutional import”); *United States v. Berkos*, 543 F.3d 392, 398 (7th Cir. 2008) (distinguishing between “substantive” and “procedural” violations of Rule 41); *United States v. Simons*, 206 F.3d 392, 403 (4th Cir. 2000) (distinguishing “constitutional” and “ministerial” violations of Rule 41).

#### A.

To demonstrate that the violation of Rule 41 was of constitutional magnitude, Werdene must show a violation of his Fourth Amendment rights. *See United States v. Martinez-Zayas*, 857 F.2d 122, 136 (3d Cir. 1988), *overruled on other grounds by United States v. Chapple*, 985 F.2d 729 (3d Cir. 1993). Specifically, he must articulate how the Government’s failure to comply with Rule 41(b) caused a search or seizure prohibited by the Fourth Amendment. He cannot do so.

Werdene does not argue that the Government violated his Fourth Amendment rights by seeking a warrant without probable cause. (Hr’g Tr. 23:16–22.) Rather, as the Government asserts, his argument is that Agent Macfarlane applied for the NIT warrant in the wrong district. (Gov’t’s Opp. at 15.) Werdene contends rather circularly that the Government’s “violation of Rule 41 is of constitutional magnitude because it did not involve mere ministerial violations of the rule.” (Def.’s Mot. at 16 (citation omitted).) He argues that the Fourth Amendment protects his use of his computer inside the privacy of his own home and “[a]llowing the Government to ignore the limits imposed by the Rule will invite further violations and undermine the core constitutional requirement that warrants particularly describe the place or places to be searched.” (*Id.* (citations omitted).)

The Supreme Court of the United States has “uniformly . . . held that the application of the Fourth Amendment depends on whether the person invoking its protection can claim a ‘justifiable,’ a ‘reasonable,’ or a ‘legitimate expectation of privacy’ that has been invaded by the government action.” *Smith v. Maryland*, 442 U.S. 735, 740 (1979) (collecting cases). That inquiry is analyzed in two parts: (1) whether the individual, through his conduct, “exhibited an actual (subjective) expectation of privacy;” and (2) whether the individual’s subjective expectation of privacy is “one that society is prepared to recognize as ‘reasonable.’” *Id.* (citations omitted).

In *Smith*, the Supreme Court addressed whether petitioner Michael Lee Smith had a reasonable expectation of privacy in the telephone numbers he dialed. 442 U.S. at 738. The government had used a pen register to record the numbers dialed from Smith’s home in order to determine if he made threatening phone calls to another individual. *Id.* at 737. The Court rejected Smith’s argument that he had a “reasonable expectation of privacy” in the numbers that

he dialed and held that the use of the pen register was, in fact, not a search. *Id.* at 742. It reasoned that “[a]ll telephone users realize that they must ‘convey’ phone numbers to the telephone companies, since it is through telephone company switching equipment that their calls are completed.” *Id.* It rejected Smith’s argument that he attempted to keep the numbers he dialed private by dialing them from his home phone because such numbers were “convey[ed] . . . to the telephone company in precisely the same way” regardless of his location. *Id.* at 743. Further, it held that Smith’s expectation of privacy was “not one that society is prepared to recognize as reasonable” because he voluntarily turned the information over to a third party, the telephone company. *Id.* at 743–44 (citing *Katz v. United States*, 389 U.S. 347, 361 (1967)) (internal quotation marks omitted).

The Third Circuit has similarly held that an individual has “no reasonable expectation of privacy in his IP address and so cannot establish a Fourth Amendment violation.” *United States v. Christie*, 624 F.3d 558, 574 (3d Cir. 2010) (citations omitted). “[N]o reasonable expectation of privacy exists in an IP address, because that information is also conveyed to and, indeed, from third parties, including [internet service providers].” *Id.*; see also *In re Nickelodeon Consumer Privacy Litig.*, No. 12-cv-07829, 2014 WL 3012873, at \*15 (D.N.J. July 2, 2014) (“Indeed, in the analogous Fourth Amendment context, email and IP addresses can be collected without a warrant because they constitute addressing information and do not necessarily reveal any more about the underlying contents of communications than do phone numbers, which can be warrantlessly captured via pen registers.”) (citation and internal quotation marks omitted); *United States v. Forrester*, 512 F.3d 500, 509–10 (9th Cir. 2008) (comparing IP addresses to the outside of a letter and the monitoring of IP addresses to a pen register). The Third Circuit in *Christie* noted that “IP addresses are not merely passively conveyed through third party

equipment, but rather are voluntarily turned over in order to direct the third party's servers." 624 F.3d. at 574 (citations and internal quotation marks omitted).

Werdene had no reasonable expectation of privacy in his IP address. Aside from providing the address to Comcast, his internet service provider, a necessary aspect of Tor is the initial transmission of a user's IP address to a third-party: "in order for a prospective user to use the Tor network they must disclose information, including their IP addresses, to unknown individuals running Tor nodes, so that their communications can be directed toward their destinations." *United States v. Farrell*, No. 15-cr-029, 2016 WL 705197, at \*2 (W.D. Wash. Feb. 23, 2016). The court in *Farrell* held that "[u]nder these circumstances Tor users clearly lack a reasonable expectation of privacy in their IP addresses while using the Tor network." *Id.*; *see also Michaud*, 2016 WL 337263, at \*7 ("Although the IP addresses of users utilizing the Tor network may not be known to websites, like [Playpen], using the Tor network does not strip users of all anonymity, because users . . . must still send and receive information, including IP addresses, through another computer . . .").<sup>6</sup>

That Werdene's IP address was subsequently bounced from node to node within the Tor network to mask his identity does not alter the analysis of whether he had an actual expectation of privacy in that IP address. In *Smith*, the petitioner argued that the numbers he dialed on his telephone remained private because they were processed through automatic switching equipment rather than a live operator. 442 U.S. at 745. The Court rejected that argument, finding that the

---

<sup>6</sup> In support of his argument, Werdene relies on *In re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753 (S.D. Tex. 2013). That case involved FBI agents seeking a warrant to install software on a computer whose location was not ascertainable. *Id.* at 755. The software could generate user records and take control of a computer's camera to generate photographs of the user. *Id.* The magistrate judge declined to issue the warrant because the jurisdictional requirements of Rule 41(b) were not met and because it violated the Fourth Amendment's particularity requirement and protections against intrusive video surveillance. *Id.* at 757-61. *In re Warrant* is distinguishable based on the intrusive and general nature of the information sought. Unlike the software in that case, the NIT targeted users who were accessing child pornography and revealed information in which they had no reasonable expectation of privacy.

telephone company's decision to use automatic equipment instead of a live operator did not "make any constitutional difference" in analyzing the petitioner's reasonable expectations of privacy. *Id.* Similarly, the type of third-party to which Werdene disclosed his IP address—whether a person or an "entry node" on the Tor network—does not affect the Court's evaluation of his reasonable expectation of privacy. He was aware that his IP address had been conveyed to a third party and he accordingly lost any subjective expectation of privacy in that information. *See Farrell*, 2016 WL 705197, at \*2 ("[T]he Tor Project [communicates to users] that the Tor network has vulnerabilities and that users might not remain anonymous.").<sup>7</sup>

## B.

Even if Werdene maintained a subjective expectation that his IP address would remain private through his use of Tor, that expectation is not "one that society is prepared to recognize as 'reasonable.'" *Katz*, 389 U.S. at 361. In *United States v. Stanley*, 753 F.3d 114 (3d Cir. 2014), Richard Stanley accessed his neighbor's wireless internet connection without permission to share child pornography. Police officers learned Stanley's IP address by analyzing the neighbor's router and located him by using a device known as a "MoocherHunter." *Id.* at 116. MoocherHunter is a mobile tracking software that is used with a directional antenna to locate a "mooching computer" by detecting the strength of the radio waves it is emitting. *Id.*

Stanley contended that the officers' use of MoocherHunter constituted a warrantless search and sought suppression of the evidence against him. *Id.* at 117. After the district court denied his motion, the Third Circuit affirmed, holding that the officers did not conduct a

---

<sup>7</sup> Werdene does not argue that he had a reasonable expectation of privacy in the other material gathered by the NIT, including the type of operating system running on the computer, his computer's active operating system username and his computer's MAC address. Nor does Werdene contend that any of that information was material to the investigation of his activities and his subsequent identification.

“search” within the meaning of the Fourth Amendment because Stanley did not have a reasonable expectation of privacy in his wireless internet signal. *Id.* at 119–22.

The Third Circuit reasoned that “while Stanley may have justifiably expected the path of his invisible radio waves to go undetected, society would not consider this expectation ‘legitimate’ given the unauthorized nature of his transmission.” *Id.* at 120 (citing *Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) (“[A] burglar plying his trade in a summer cabin during the off season may have a thoroughly justified subjective expectation of privacy, but it is not one which the law recognizes as ‘legitimate.’”)); *see also United States v. Jacobson*, 466 U.S. 109, 122 (1984) (“The concept of an interest in privacy that society is prepared to recognize as reasonable is, by its very nature, critically different from the mere expectation, however well justified, that certain facts will not come to the attention of the authorities.”). Werdene’s use of Tor to view and share child pornography is not only an activity that society rejects, but one that it seeks to sanction. *See, e.g.,* Providing Resources, Officers, and Technology to Eradicate Cyber Threats to Our Children Act of 2008, 42 U.S.C. §§ 17611, 17612 (authorizing the Attorney General to create a National Strategy for Child Exploitation Prevention and Interdiction and establishing a National Internet Crimes Against Children Task Force Program); *Stanley*, 753 F.3d at 121 (concluding that society would be unwilling to recognize Stanley’s privacy interests as “reasonable” where “the purpose of [his] unauthorized connection was to share child pornography”).

The Third Circuit further stated in *Stanley* that recognizing his expectation of privacy as “legitimate” would “reward him for establishing his Internet connection in such an unauthorized manner.” 753 F.3d at 121. Here, Werdene seeks to “serendipitously receive Fourth Amendment protection” because he used Tor in an effort to evade detection, even though an individual who

does not conceal his IP address does not receive those same constitutional safeguards. *Id.* (citing *United States v. Broadhurst*, No. 11-cr-00121, 2012 WL 5985615, at \*5 (D. Or. Nov. 28, 2012)). Since Werdene did not have a reasonable expectation of privacy in his IP address, the NIT cannot be considered a “search” within the meaning of the Fourth Amendment and the violation at issue is therefore not constitutional. *See Martinez-Zayaz*, 857 F.2d at 136.

#### IV.

Werdene is left to contend that suppression is warranted even if the Government’s violation of Rule 41 was nonconstitutional, procedural or “ministerial.” (Def.’s Mem. at 16–17.) He relies on the Tenth Circuit Court of Appeals’s suppression standard in the context of a nonconstitutional Rule 41 violation. Specifically, in *United States v. Krueger*, 809 F.3d 1109 (10th Cir. 2015), the Tenth Circuit stated that it:

consider[s] whether the defendant can establish that, as a result of the Rule violation (1) there was prejudice in the sense that the search might not have occurred or would not have been so abrasive if the Rule had been followed, or (2) there is evidence of intentional and deliberate disregard of a provision of the Rule.

*Id.* at 1114.<sup>8</sup> Werdene claims he was prejudiced because the NIT “would not have occurred[] but for the Rule 41 violation.” (Def.’s Mem. at 17.) He also contends that the Government “acted with intentional and deliberate disregard of Rule 41” as the Rule “simply does not permit remote, dragnet searches of computers outside of the authorizing district.” (*Id.*)

---

<sup>8</sup> In *Krueger*, the Tenth Circuit adopted the Ninth Circuit’s suppression standard for nonconstitutional violations of Rule 41 first articulated in *United States v. Stefanson*, 648 F.2d 1231, 1235 (9th Cir. 1981). Several other circuits also use the *Stefanson* test. *See, e.g., United States v. Comstock*, 805 F.2d 1194, 1207 (5th Cir. 1986); *United States v. Loyd*, 721 F.2d 331, 333 (11th Cir. 1983); *United States v. Gitcho*, 601 F.2d 369, 372 (8th Cir. 1979), *cert. denied*, 444 U.S. 871 (1979); *United States v. Mendel*, 578 F.2d 668, 673–74 (7th Cir. 1978), *cert. denied*, 439 U.S. 964 (1978).



The Third Circuit defines prejudice differently than the Tenth Circuit.<sup>9</sup> In the Third Circuit, a nonconstitutional violation of Rule 41 warrants suppression when it “caused prejudice or was done with intentional and deliberate disregard of the rule’s requirements.” *United States v. Cox*, 553 F. App’x 123, 128 (3d Cir. 2014); *see also United States v. Slaey*, 433 F. Supp. 2d 494, 498 (E.D. Pa. 2006). Our Circuit defines prejudice “in the sense that it offends concepts of fundamental fairness or due process.” *Hall*, 505 F.2d at 964; *see also United States v. Searp*, 586 F.2d 1117, 1125 (6th Cir. 1978) (“The Third Circuit has adopted a similar, but more restrictive ‘prejudice’ test, requiring suppression ‘only when the defendant demonstrates prejudice from the Rule 41 violation . . . in the sense that it offends concepts of fundamental fairness or due process.’”) (quoting *Hall*, 505 F.2d at 961); *United States v. Burka*, 700 F. Supp. 825, 830 (E.D. Pa. 1988) (articulating *Hall*’s prejudice standard). The Government’s actions in this case do not offend notions of fundamental fairness or due process.

After assuming control of Playpen and moving its server to a government facility in Newington, Virginia, Agent Macfarlane sought and obtained a warrant to employ the NIT in the Eastern District of Virginia. (Gov’t’s Opp., Ex. 1 ¶¶ 28, 30.) Before activating the NIT, Agent Macfarlane did not—and could not—know that Werdene resided in the Eastern District of Pennsylvania. Indeed, the only way in which the Government could have procedurally complied with Rule 41 was either through sheer luck (*i.e.*, Werdene’s location happened to be within the Eastern District of Virginia) or by applying for a warrant in every one of the ninety-four federal judicial districts. Agent Macfarlane’s warrant application, which was approved by a neutral and

---

<sup>9</sup> The Government also argues that *Krueger*’s facts are distinguishable from this case. (Gov’t’s Opp. at 17.) In *Krueger*, Homeland Security Investigations (“HIS”) agents sought and obtained a warrant from a magistrate judge in the District of Kansas to search properties in Oklahoma. *See United States v. Krueger*, 809 F.3d 1109, 1111 (10th Cir. 2015). There, it was clear in which district the HIS agents should have made their warrant request. Here, however, Werdene’s use of Tor to mask his IP address obscured his location from FBI agents. Unlike *Krueger*, the FBI agents could not know Werdene’s location prior to requesting the warrant.

detached magistrate judge, described the NIT process in copious detail. (*See generally* Gov't's Opp., Ex. 1.) The warrant application states that the NIT would deploy "each time that any user or administrator log[ged] into Playpen by entering a username and password." (*Id.*, Ex. 1 ¶ 36.) This enabled the FBI to link a username and its corresponding activity to an IP address. (*Id.*, Ex. 1 ¶ 37.) Agent Macfarlane specifically noted that the NIT could enable this process on users of Playpen "wherever located." (*Id.*, Ex. 1 ¶ 46.) The Government's nonconstitutional violation of Rule 41 does not offend concepts of fundamental fairness or due process and Werdene's motion to suppress cannot be granted on prejudice grounds. *See United States v. McMillion*, No. 08-cr-0205, 2011 WL 9110, at \*4 (M.D. Pa. Jan. 3, 2011), *aff'd*, 472 F. App'x 138 (3d Cir. 2012).

## B.

Werdene also contends that the Government acted with intentional and deliberate disregard of Rule 41 because the FBI misled the magistrate judge "with respect to the true location of the activating computers to be searched." (Def.'s Mem. at 17.) Werdene claims that this was "egregious[] because it is a deliberate flaunting of the Rule[.]" (Hr'g Tr. 33:2-3.) A review of the record, and specifically Agent Macfarlane's warrant application, shows no deception on the Government's part. The warrant request was candid about the challenge that the Tor network poses, specifically its ability to mask a user's physical location. (Gov't's Opp., Ex. 1 ¶¶ 28, 30.) Agent Macfarlane stated that the NIT would be deployed "each time" that "any user" logged into Playpen "wherever" they were "located." (*Id.*, Ex. 1 ¶ 46.) As discussed *infra*,

Section V.D., the Government did not mislead the magistrate judge but was instead up front about the NIT's method and scope.<sup>10</sup>

## V.

Even if Werdene had a reasonable expectation of privacy in the information obtained by the NIT—rendering the Rule 41(b) violation constitutional in nature—suppression is not the appropriate remedy.

### A.

When the Government seeks to admit evidence collected pursuant to an illegal search or seizure, the exclusionary rule operates to suppress that evidence and makes it unavailable at trial. *See United States v. Katzin*, 769 F.3d 163, 169 (3d Cir. 2014) (en banc), *cert. denied*, 135 S. Ct. 1448 (2015) (citing *Herring v. United States*, 555 U.S. 135, 139 (2009)). The exclusionary rule was developed “[t]o deter Fourth Amendment violations.” *Id.*

Whether suppression is appropriate under the exclusionary rule is a separate question from whether a defendant's Fourth Amendment rights were violated. *See Hudson v. Michigan*, 547 U.S. 586, 591–92 (2006); *accord Herring*, 555 U.S. at 140. Exclusion is not a personal right conferred by the Constitution and was not “designed to ‘redress the injury’ occasioned by an unconstitutional search.” *Davis v. United States*, 564 U.S. 229, 236 (2011) (quoting *Stone v. Powell*, 428 U.S. 465, 486 (1976)). Rather, the exclusionary rule is “a judicially created means of effectuating the rights secured by the Fourth Amendment.” *Stone*, 428 U.S. at 482. The fact that a Fourth Amendment violation occurs does not mean that the evidence is automatically

---

<sup>10</sup> Werdene also argues that the Government violated Rule 41's notice requirement. (Def.'s Mem. at 18–20.) A careful reading of Agent Macfarlane's warrant application, however, shows that he requested the delay of any notice for up to 30 days under Rule 41(f)(3) and 18 U.S.C. § 3103(a)(b)(1) and (3) to avoid any tampering with Playpen while the investigation was ongoing. (Gov't's Opp., Ex. 1 ¶¶ 38–41.) He also noted that due to the anonymity of Playpen's users, “the investigation has not yet identified an appropriate person to whom such notice can be given.” (*Id.*, Ex. 1 ¶ 40.) Regardless, even if the notice requirement was violated, suppression is not an appropriate remedy because he was not prejudiced by the violation. *See supra* Section IV.A.

suppressed. *See Katzin*, 769 F.3d at 170 (citing *Herring*, 555 U.S. at 140). Indeed, “exclusion ‘has always been our last resort, not our first impulse.’” *Herring*, 555 U.S. at 140 (quoting *Hudson*, 547 U.S. at 591).

Application of the rule is instead “limited to those ‘unusual cases’ in which it may achieve its objective: to appreciably deter governmental violations of the Fourth Amendment.” *Katzin*, 769 F.3d at 170 (quoting *Leon*, 468 U.S. at 909). “Real deterrent value” alone, however, is insufficient for the exclusionary rule to apply. *Id.* at 171 (quoting *Davis*, 564 U.S. at 237). The deterrent value must also outweigh the “substantial social costs” of exclusion. *Leon*, 468 U.S. at 907. Such costs “often include omitting ‘reliable, trustworthy evidence’ of a defendant’s guilt, thereby ‘suppress[ing] the truth and set[ting] [a] criminal loose in the community without punishment.’” *Katzin*, 769 F.3d at 171 (quoting *Davis*, 564 U.S. at 237). Because this result runs contrary to the truth-finding functions of judge and jury, “exclusion is a bitter pill, swallowed only as a last resort.” *Id.* (citations and internal quotation marks omitted). Accordingly, exclusion is warranted “where the deterrent value of suppression . . . overcome[s] the resulting social costs.” *Id.* (citing *Davis*, 564 U.S. at 237).

The good faith exception to the exclusionary rule “was developed to effectuate this balance and has been applied ‘across a range of cases.’” *Id.* (quoting *Davis*, 564 U.S. at 238). *Leon* and its progeny highlight that “the deterrence benefits of exclusion ‘var[y] with the culpability of the law enforcement conduct’ at issue.” *Davis*, 564 U.S. at 238 (quoting *Herring*, 555 U.S. at 143). The deterrent value of suppression tends to outweigh the costs “[w]here officers exhibit ‘deliberate,’ ‘reckless,’ or ‘grossly negligent’ disregard for Fourth Amendment rights.” *Id.* (quoting *Herring*, 555 U.S. at 144). When the police act with an “objectively reasonable good-faith belief” in the legality of their conduct, or when their conduct “involves

only simple, isolated negligence, the deterrence rationale loses much of its force, and exclusion cannot pay its way.” *Id.* (citations and internal quotation marks omitted). Accordingly, discerning “whether the good faith exception applies requires courts to answer the ‘objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal in light of all of the circumstances.’” *Katzin*, 769 F.3d at 171 (quoting *Herring*, 555 U.S. at 145).

### B.

Werdene relies on *United States v. Levin*, No. 15-cr-10271, 2016 WL 2596010 (D. Mass. May 5, 2016). In that case, the United States District Court for the District of Massachusetts addressed whether the NIT was a substantive or procedural violation of Rule 41 and whether the information obtained from the NIT should be suppressed. The court held, in relevant part, that: (1) the NIT warrant constituted a “substantive” or constitutional violation of Rule 41(b) in that it infringed on the defendant’s Fourth Amendment rights; and (2) that the good faith exception was not available in this context, *i.e.*, where a magistrate judge issued a warrant without proper jurisdiction. *Id.*

In finding that the NIT warrant was a substantive violation of Rule 41(b), the *Levin* court reasoned that “the violation here involved ‘substantive judicial authority’ rather than simply ‘the procedures for obtaining and issuing warrants.’” *Id.* at \*8 (quoting *Krueger*, 809 F.3d at 1115). The court “assume[d] that [the defendant] had a reasonable expectation of privacy as to the information obtained through the execution of the various warrants.” *Id.* at \*1 n.1. The court in *Levin* held that because Rule 41(b) “did not grant [the magistrate] authority to issue the NIT warrant . . . [she] was without jurisdiction to do so.” *Id.* at \*8.

The court went further, concluding that this jurisdictional flaw rendered the warrant “void *ab initio*.” *Id.* (citing, *inter alia*, *United States v. Master*, 614 F.3d 236, 241 (6th Cir. 2010)). It then stated that a warrant “void *ab initio*” was equivalent to “no warrant at all.” *Id.* at \*12. The court likened this situation to a “warrantless search” scenario which is “presumptively unreasonable” under the Fourth Amendment, and accordingly found a “substantive” or constitutional violation of Rule 41(b). *Id.* at \*12 (citing *United States v. Curzi*, 867 F.2d 36 (1st Cir. 1989)).

The court also held that the good faith exception was not available in cases where a warrant was void *ab initio* and, therefore granted the motion to suppress. *Id.* at \*10–13. In doing so, it relied on the Sixth Circuit Court of Appeals’s decision in *United States v. Scott*, 260 F.3d 512 (6th Cir. 2001). The *Levin* court stated that while “the Supreme Court has expanded the good-faith exception to contexts beyond those *Leon* specifically addressed,” none of those cases “involved a warrant that was void *ab initio*, and therefore none direct the conclusion that the good-faith exception ought apply to this case.” *Levin*, 2016 WL 2596010, at \*11.

### C.

*Levin*’s reliance on *Scott* was misplaced, particularly given the court’s acknowledgement that “the Sixth Circuit effectively reversed [*Scott*]” in *United States v. Master*, 614 F.3d 236 (6th Cir. 2010).<sup>11</sup> *Id.* at \*11; *see also United States v. Beals*, 698 F.3d 248, 265 (6th Cir. 2012) (recognizing that *Master* overruled *Scott*). In *Master*, the Sixth Circuit reexamined its holding in

<sup>11</sup> *Levin* later noted that “[e]ven in *Master* . . . the court acknowledged that the recent Supreme Court cases addressing the good-faith exception ‘do [ ] not directly overrule our previous decision in *Scott*.’” *Levin*, 2016 WL 2596010, at \*12 (citing *Master*, 614 F.3d at 243). It is therefore unclear whether or not *Levin* believed *Scott* was overruled. In any event, *Master* provided that “nothing in this opinion should cast doubt on the ultimate outcome in *Scott*. In that case, the officers made at best minimal attempts to find available, active magistrates before presenting the warrant to the retired judge.” *Master*, 614 F.3d at 242 n.3. Thus, *Master* simply noted that the officers’ actions in *Scott*, analyzed under the newly adopted good faith framework, fell below the standard necessary to apply the good faith exception to the exclusionary rule. To the extent *Levin* seeks to rely on *Master*’s footnote for the proposition that the good faith exception is inapplicable in this context, such a finding was clearly rejected by *Master*.

*Scott*—that the good faith exception could never apply where a warrant was void *ab initio*—in light of the Supreme Court’s decisions in *Herring* and *Hudson*. 614 F.3d at 242–43. *Master* found *Herring*’s separation of the suppression and Fourth Amendment violation inquiries to be “contrary to a foundational assumption of the opinion in *Scott* that: ‘Subject to a few exceptions, the exclusionary rule requires the suppression of evidence obtained in violation of the Fourth Amendment.’” *Id.* at 242 (quoting *Scott*, 260 F.3d at 514). The court stated:

Whereas *Scott* effectively required the government to qualify for an exception to the general rule of suppression, the Supreme Court has since emphasized that the decision to exclude evidence is divorced from whether a Fourth Amendment violation occurred. The exclusionary rule’s purpose is instead to deter deliberate, reckless, or grossly negligent conduct, or in some circumstances recurring or systemic negligence.

*Id.* (citations and internal quotation marks omitted). The Sixth Circuit accordingly found that the good faith exception *could* apply in situations where the warrant was void *ab initio*. *See id.* at 242–43.

Rather than rely on *Master*, the court in *Levin* instead deferred to *Scott*, stating that “[t]he *Master* court read the Supreme Court’s recent good-faith cases too broadly.” *Levin*, 2016 WL 2596010, at \*12. The court explained its reasoning in a footnote, stating that while *Herring* “makes much of the connection between the exclusionary rule and the goal of deterrence and culpability of law enforcement . . . it says nothing about whether the same calculus ought apply where there was never jurisdiction to issue a valid warrant in the first place.” *Id.* at \*12 n.22. *Levin* apparently discounted *Master*’s reliance on *Herring* because *Herring* did not hold that the good faith exception applies where a warrant was void *ab initio*, *i.e.*, it never dealt with an issue that *Levin* admits was one of “first impression in this Circuit, and an unresolved question more broadly.” *Id.* at \*10. *But see United States v. Knights*, 534 U.S. 112, 117 (2001) (criticizing as “dubious logic” the argument “that an opinion upholding the constitutionality of a particular

search implicitly holds unconstitutional any search that is not like it”); *Arizona v. Evans*, 514 U.S. 1, 13 (1995) (“Subsequent case law has rejected [a] reflexive application of the exclusionary rule.”) (citation omitted).

The Third Circuit has emphasized that courts “must be prepared to apply th[e] good-faith exception across a range of cases.” *Katzin*, 769 F.3d at 178 (quoting *Davis*, 564 U.S. at 238) (internal quotation marks omitted). Indeed, the court in *Katzin* found that the good faith exception applied in the context of a warrantless search where the officers “acted . . . upon an objectively reasonable good faith belief in the legality of their conduct.” *Id.* at 182. Moreover, it explicitly rejected the appellees’ argument that it would be “fabricat[ing] a new good faith ground,” stating that while “[t]he factual circumstances before us differ, [] we ground our application of the good faith exception in the same time-tested considerations.” *Id.* at 178 n.11. In other words, the legal status of the warrant under the Fourth Amendment does not inform the decision of whether the good faith exception is available in a given case; that inquiry is separate and must be considered in light of the exclusionary rule’s purpose and the officers’ conduct at issue. *See Master*, 614 F.3d at 243.

Additionally, as *Master* indicates, “the exclusionary rule was crafted to curb police rather than judicial misconduct.” *Id.* at 242 (citation omitted). Arguably, the magistrate judge’s lack of authority to issue the warrant has no impact on police misconduct. *See id.* Applying the rule here without exception makes little sense where it was the magistrate, not the agents, who determined that she had jurisdiction. *See, e.g., Emp’rs Ins. of Wausau v. Crown Cork & Seal Co.*, 905 F.2d 42, 45 (3d Cir. 1990) (“A federal court is bound to consider its own jurisdiction preliminary to consideration of the merits.”) (quoting *Trent Realty Assocs. v. First Fed. Sav. & Loan Ass’n of Phila.*, 657 F.2d 29, 36 (3d Cir. 1981)); *In re Warrant to Search a Target*



*Computer at Premises Unknown*, 958 F. Supp. 2d 753, 757 (S.D. Tex. 2013) (declining to issue a warrant under Rule 41(b) because, *inter alia*, the court lacked jurisdiction). The good faith exception is not foreclosed in the context of a warrant that is void *ab initio* and the Court must now determine if it applies.

**D.**

The question is whether “the agents acted with a good faith belief in the lawfulness of their conduct that was ‘objectively reasonable.’” *Katzin*, 769 F.3d at 182 (quoting *Davis*, 564 U.S. at 238). The Court must consider all of the circumstances and confine its inquiry to the “objectively ascertainable question whether a reasonably well trained officer would have known that the search was illegal in light of that constellation of circumstances.” *Katzin*, 769 F.3d at 182 (quoting *Leon*, 468 U.S. at 922 n.23) (internal quotation marks omitted).

The agents in this case acted upon an objectively reasonable good faith belief in the legality of their conduct. Attachment A to the warrant application is titled “Place to be Searched” and specifically authorizes deployment of the NIT to “activating computers.” (Gov’t Opp., Ex. 1 Attach A.) “Activating computers” are defined as “those of any user or administrator who logs into [Playpen] by entering a username and password.” (*Id.*) Attachment A notes that the Eastern District of Virginia is where the NIT will be deployed. (*Id.*) Thus, an “objectively reasonable” reading of the warrant gave the agents “authority to deploy the NIT from a government-controlled computer in the Eastern District of Virginia against anyone logging onto Website A, with any information gathered by the NIT to be returned to the government-controlled computer in the Eastern District of Virginia.” *United States v. Michaud*, No. 15-cr-05351, 2016 WL 337263, at \*4 (W.D. Wash. Jan. 28, 2016).

Werdene claims that the Government acted with intentional and deliberate disregard of Rule 41 because the FBI misled the magistrate judge “with respect to the true location of the activating computers to be searched.” (Def.’s Mem. at 17.) This argument is belied by both the warrant and warrant application. Agent Macfarlane stated in the warrant application that the “NIT may cause an activating computer—*wherever located*—to send to a computer controlled by or known to the government, network level messages containing information that may assist in identifying the computer, *its location*, other information about the computer and the user of the computer.” (Gov’t Opp., Ex. 1 ¶ 46 (emphasis added).) With this information, the magistrate judge believed that she had jurisdiction to issue the NIT warrant. Contrary to Werdene’s assertion, this is not a case where the agents “hid the ball” from the magistrate or misrepresented how the search would be conducted. *See, e.g., Illinois v. Gates*, 462 U.S. 213, 264 (1983) (“Similarly, the good-faith exception would not apply if the material presented to the magistrate or judge is false or misleading.”) (citing *Franks v. Delaware*, 438 U.S. 154 (1978)).

While the *Levin* court found the good faith exception foreclosed in this scenario, it alternatively held that if the exception did apply, suppression was nonetheless appropriate. *See Levin*, 2016 WL 2596010, at \*13. The court reasoned that “it was not objectively reasonable for law enforcement—particularly a veteran FBI agent with 19 years of federal law enforcement experience—to believe that the NIT Warrant was properly issued considering the plain mandate of Rule 41(b).” *Id.* (citations and internal quotation marks omitted). Noting that “the conduct at issue here can be described as systemic error or reckless disregard of constitutional requirements,” the court found suppression appropriate. *Id.* (citations and internal quotation marks omitted).

The court in *Levin* did not analyze the “costs” associated with suppression. The Supreme Court has stated that these costs are “substantial,” *Leon*, 468 U.S. at 907, given that suppression “often excludes ‘reliable, trustworthy evidence’ of a defendant’s guilt, ‘suppress[es] the truth and set[s] [a] criminal loose in the community without punishment.’” *Katzin*, 769 F.3d at 186 (quoting *Davis*, 564 U.S. at 237). The court in *Levin* also did not address what deterrent effect, if any, suppression would have in this case. While the court found that the agents’ conduct constituted “systemic error or [a] reckless disregard of constitutional requirements,” it failed to address why that is the case. *Levin*, 2010 WL 2596010, at \*13. *Levin* seemed to overlook the Supreme Court’s directive that “the exclusionary rule is not an individual right and applies only where it result[s] in appreciable deterrence.” *Herring*, 555 U.S. at 141 (quoting *Leon*, 468 U.S. at 909).

Further, to the extent a mistake was made in this case, it was not made by the agents in “reckless . . . disregard for Fourth Amendment rights.” *Davis*, 564 U.S. at 238 (quoting *Herring*, 555 U.S. at 144). Rather, it was made by the magistrate when she mistakenly issued a warrant outside her jurisdiction. The agents consulted with federal attorneys before preparing the warrant application. (Gov’t’s Opp. at 24.) *See e.g.*, *Katzin*, 769 F.3d at 181 (stating that “[w]e have previously considered reliance on government attorneys in our good faith calculus and concluded that, based upon it in combination with other factors, ‘[a] reasonable officer would . . . have confidence in [a search’s] validity’”) (quoting *United States v. Tracey*, 597 F.3d 140, 153 (3d Cir. 2010)). They presented the magistrate judge with all relevant information to allow her to make a decision as to whether Rule 41(b) permitted her to issue the warrant. The FBI agents did not misrepresent how the search would be conducted or, most importantly, where it would be conducted.

A magistrate judge's mistaken belief that she had jurisdiction, absent any indicia of reckless conduct by the agents, does not warrant suppression. The Supreme Court has stated:

To the extent . . . proponents of exclusion rely on its behavioral effects on judges and magistrates in these areas, their reliance is misplaced . . . . [T]here exists no evidence suggesting that judges and magistrates are inclined to ignore or subvert the Fourth Amendment or that lawlessness among these actors requires application of the extreme sanction of exclusion . . . . And, to the extent that the rule is thought to operate as a "systemic" deterrent on a wider audience, it clearly can have no such effect on individuals empowered to issue search warrants. Judges and magistrates are not adjuncts to the law enforcement team; as neutral judicial officers, they have no stake in the outcome of particular criminal prosecutions. The threat of exclusion thus cannot be expected significantly to deter them.

*Leon*, 468 U.S. at 916–17. Exclusion of the evidence in this case would only serve to "punish the errors of judges and magistrates" and would not have any "appreciable" effect on law enforcement. *Id.* at 909, 916.

Had the agents lied to the magistrate and told her that all the information being sought would be gathered only in the Eastern District of Virginia, the Court's analysis would likely change because suppression deters misrepresentations made to the Court. *See, e.g., Franks*, 438 U.S. at 171 (finding exclusion appropriate where there is proof of "deliberate falsehood or of reckless disregard for the truth"). In this case, however, the agents provided the magistrate with all the information she needed to "satisfy [herself] of [her] jurisdiction before proceeding . . . ." *Packard v. Provident Nat'l Bank*, 994 F.2d 1039, 1049 (3d Cir. 1993) (citations omitted). Once the warrant was issued, albeit outside the technical bounds of Rule 41(b), the agents acted upon an objectively reasonable good faith belief in the legality of their conduct. *Cf. Leon*, 468 U.S. at 921 ("In the ordinary case, an officer cannot be expected to question the magistrate's . . . judgment that the form of the warrant is technically sufficient . . . . Penalizing the officer for the

magistrate’s error, rather than his own, cannot logically contribute to the deterrence of Fourth Amendment violations.”).

Here, as in *Katzin*, “the Government’s evidence against [the defendant] is substantial, and it is uncontested that the Government would have no case without it.” *Katzin*, 769 F.3d at 186. The “cost” of suppression, therefore, would be letting a “guilty and possibly dangerous defendant[] go free—something that ‘offends basic concepts of the criminal justice system.’” *Herring*, 555 U.S. at 141 (quoting *Leon*, 468 U.S. at 908). Absent any appreciable deterrent effect on law enforcement, suppression would only serve to “exact[] a heavy toll on both the judicial system and society at large.” *Davis*, 564 U.S. at 237.

An appropriate order follows.

BY THE COURT:

/s/ Gerald J. Pappert  
GERALD J. PAPPERT, J.



# CONSTITUTIONAL MALWARE

Jonathan Mayer<sup>\*</sup>

*The United States government hacks computer systems, for law enforcement purposes. According to public disclosures, both the Federal Bureau of Investigation and Drug Enforcement Administration are increasingly resorting to computer intrusions as an investigative technique. This article provides the first comprehensive examination of how the Constitution should regulate government malware.*

*When applied to computer systems, the Fourth Amendment safeguards two independent values: the integrity of a device as against government breach, and the privacy properties of data contained in a device. Courts have not yet conceptualized how these theories of privacy should be reconciled.*

*Government malware forces a constitutional privacy reckoning. Investigators can algorithmically constrain the information that they retrieve from a hacked device, ensuring they receive only data that is—in isolation—constitutionally unprotected. According to declassified documents, FBI officials have theorized that the Fourth Amendment does not apply in this scenario. A substantially better view of the law, I conclude, is that the Fourth Amendment’s dual protections are cumulative, not mutually exclusive.*

*Applying this two-stage framework, I find that the Fourth Amendment imposes a warrant requirement on almost all law enforcement malware. The warrant must be valid throughout the duration of the malware’s operation, and must provide reasonable ex post notice to a computer’s owner. In certain technical configurations, the Constitution goes even further, requiring law enforcement to satisfy an exacting “super-warrant” standard. Reviewing public disclosures, I find that the government has a spotty record of compliance with these foundational privacy safeguards.*

*Moving beyond established doctrine and current practice, I normatively argue that the super-warrant standard should apply to government hacking. The same considerations that prompted heightened judicial review of wiretapping in the 1960s should prompt close scrutiny of law enforcement malware today.*

---

<sup>\*</sup> J.D., Stanford Law School, 2013; Ph.D., Stanford University Department of Computer Science, Expected 2015. The author is deeply grateful to the agents of the Federal Bureau of Investigation and the attorneys of the Department of Justice attorneys who shared their views on government hacking. This work draws upon conversations at the Privacy Law Scholars Conference and the Rethinking Privacy and Surveillance in the Digital Age event at Harvard Law School.

INTRODUCTION .....	2
I. DOES THE FOURTH AMENDMENT PROTECT DEVICES OR DATA? .....	5
A. <i>A Device-Centric Theory</i> .....	7
B. <i>A Data-Centric Theory</i> .....	8
C. <i>Reconciling the Two Theories</i> .....	10
1. Solely the Device-Centric Theory .....	10
2. The Lesser Protection of the Two Theories .....	11
3. Solely the Data-Centric Theory .....	12
4. The Greater Protection of the Two Theories .....	18
II. EVALUATING THE CONSTITUTIONALITY OF MALWARE .....	21
A. <i>When does government access become a search?</i> .....	22
B. <i>How do probable cause and particularity apply to government hacking?</i> .....	25
C. <i>Does government malware require a continuously valid warrant?</i> ..	30
D. <i>When and how must the government provide notice of hacking?</i> .....	34
E. <i>When does government malware require a super-warrant?</i> .....	38
CONCLUSION: IN FAVOR OF MALWARE SUPER-WARRANTS .....	40

## INTRODUCTION

Timberline High School was gripped by panic.<sup>1</sup> In the span of just over a week, the suburban school had received *nine* anonymous bomb threats—prompting repeated evacuations and police sweeps.<sup>2</sup> The perpetrator taunted academic administrators with a litany of emails, and he spooked students from a threatening social network account.<sup>3</sup> He also knocked campus computer systems offline.

Local police and the county sheriff were stumped. They had obtained information about the perpetrator’s network access and accounts—but the traffic was routed through Italy, and the names were all fake. After exhausting their conventional investigative tools, they called in the Federal Bureau of Investigation.

One week later, FBI agents hacked the hoaxster’s computer. They sent a

---

<sup>1</sup> See Timberline High School, *Letter to the Timberline Community*, KIRO 7, June 14, 2007, <http://www.kirotv.com/news/news/letter-from-timberline-high-school/nKbdy/>.

<sup>2</sup> *Lacey 10th-Grader Arrested in Threats to Bomb School*, SEATTLE TIMES, June 14, 2007, <http://www.seattletimes.com/seattle-news/lacey-10th-grader-arrested-in-threats-to-bomb-school/>.

<sup>3</sup> See Application and Affidavit of FBI Special Agent Norman B. Sanders for a Computer and Internet Protocol Address Verifier Warrant, No. MJ07-5114, at 6-12 (W.D. Wash. June 12, 2007).



fake *Seattle Times* article, pandering to his ego. He took the bait. When he loaded the news story, he also silently installed FBI malware.

At 2am the next day, local police raided a teenage student's home. They discovered incriminating evidence, and he admitted culpability.

\* \* \*

Law enforcement malware is not new.<sup>4</sup> The earliest reported case is from 2001, when FBI agents snuck into a Mafioso's home and installed a system for recording keystrokes.<sup>5</sup>

What's more, law enforcement agencies are increasingly resorting to malware.<sup>6</sup> It is now technically trivial to frustrate conventional computer forensic techniques, including by running anonymizing software, renting computer hardware outside the United States, or encrypting the physical data stored on a device. The defendant in the Timberline case, for instance, was just fifteen years old.

Government malware usage has also extended beyond computer-specific crimes, reaching traditionally offline misconduct. The 2001 opinion arose from an investigation of a gambling and loansharking conspiracy; subsequent malware deployments have been associated with harassment, extortion, fraud, and child pornography investigations.<sup>7</sup>

Law enforcement hacking has become so commonplace, in fact, that the

---

<sup>4</sup> I use the term "malware" throughout this article since, in the computer security field, it is the common term for software that subverts a user's device. The term is not intended as a criticism of government hacking. On the contrary, my view is that hacking can be a legitimate and effective law enforcement technique. I also use the term to promote consistency and avoid ambiguity. Government documents have referred to hacking with a wide variety of terms, including Network Investigative Technique (NIT), Computer and Internet Protocol Address Verifier (CIPAV), Internet Protocol Address Verifier (IPAV), Remote Access Search and Surveillance (RASS), Remote Computer Search, Remote Search, Web Bug, Sniffer, Computer Tracer, Internet Tracer, and Remote Computer Trace.

<sup>5</sup> *United States v. Scarfo*, 180 F. Supp. 2d 572 (D.N.J. 2001). The *Scarfo* opinion provides only a summary of the FBI's "Key Logger System," recognizing it as protected from disclosure under the Classified Information Procedures Act. What details are included suggest a design with both hardware and software components.

<sup>6</sup> See Letter from Acting Assistant Attorney General Mythili Raman to the Advisory Committee on the Federal Rules of Criminal Procedure, at 1 (Sept. 18, 2013) (describing government hacking practices as "increasingly common situations"); Email from [Redacted] to [Redacted] Re [Redacted] (Mar. 7, 2002), available at <https://www.eff.org/document/fbicipav-05pdf> ("we are seeing indications that [the Internet Protocol Address Verifier (IPAV)] technique is being used needlessly by some agencies").

<sup>7</sup> An archive of FBI documents, released under the Freedom of Information Act, includes a diverse range of requests for hacking assistance. See *Elect. Frontier Found., Endpoint Surveillance Tools*, at 10:1-19, 13:1-20 (Apr. 20, 2011), <https://www.eff.org/foia/foia-endpoint-surveillance-tools-cipav>.

federal judiciary is considering new rule provisions that expressly address the practice.<sup>8</sup> In early 2015, the Advisory Committee on the Rules of Criminal Procedure recommended malware-specific venue rules for issuing warrants.

Given the history of government hacking, its uptick in frequency, its increasing use to investigate conventional crimes, and its pending judicial rules, one might imagine a rich literature on the subject. After scouring legal databases and news reports, though, I identified just five public court orders,<sup>9</sup> four judicial opinions,<sup>10</sup> and scant scholarly treatment.<sup>11</sup> This article aims to begin filling the analytical void, offering guidance for the courts and opening a dialogue with policymakers and scholars.<sup>12</sup>

---

<sup>8</sup> See Judicial Conference of the United States, Advisory Committee on the Rules of Criminal Procedure, Proposed Amendments to the Federal Rules of Criminal Procedure, Regulations.gov, <http://www.regulations.gov/#!docketDetail;D=USC-RULES-CR-2014-0004> (last visited July 14, 2015).

<sup>9</sup> Second Amended Application and Third Amended Affidavit of FBI Task Force Officer William A. Gallegos for a Network Investigative Technique Warrant, No. 12-sw-05685-KMT (D. Colo. Dec. 11, 2013); Application and Affidavit of FBI Special Agent Justin E. Noble for a Network Investigative Technique Warrant, No. 1:12-mj-00748-ML (W.D. Tex. Dec. 18, 2012); Application and Affidavit of FBI Special Agent Jeffrey Tarpinian for a Network Investigative Technique Warrant, No. 8:12MJ356 (D. Neb. Nov. 16, 2012); Application and Affidavit of FBI Special Agent Norman B. Sanders for a Computer and Internet Protocol Address Verifier Warrant, No. MJ07-5114, at 6-12 (W.D. Wash. June 12, 2007); In Re Application for an Order Authorizing Surreptitious Entry, Mag. No. 99-4061 (D.N.J. June 9, 1999). A recent District Court opinion provides excerpts of a sixth hacking warrant application. In Re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753 (S.D. Tex. 2013).

<sup>10</sup> United States v. Pierce, No. 8:13CR106, 2014 U.S. Dist. LEXIS 147114 (D. Neb. Oct. 14, 2014) (allowing computer identification malware for visitors to child pornography websites); United States v. Pierce, No. 8:13CR106, 2014 U.S. Dist. LEXIS 108171 (D. Neb. July 28, 2014) (magistrate recommendation in same prosecution); In Re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753 (S.D. Tex. 2013) (denying a warrant for a computer behind anonymizing software, rendering its location unknown); United States v. Scarfo, 180 F. Supp. 2d 572 (D.N.J. 2001) (allowing a keylogger pursuant to a search warrant).

<sup>11</sup> See generally Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1 (2014) (overview by computer scientists of policy considerations associated with a shift from conventional wiretapping to law enforcement hacking); Nathan E. Carrell, Note, *Spying on the Mob*, 2002 U. ILL. J.L. TECH. & POL'Y 193 (2002) (reviewing *Scarfo* and arguing that keystroke monitoring should require a super-warrant); Neal Hartzog, Note, *The "Magic Lantern" Revealed*, 20 J. MARSHALL. J. INFO. TECH. & PRIV. L. 287 (2002) (arguing that *Scarfo* was rightly decided); Benjamin Lawson, Note, *What Not to "Ware"*, 35 RUTGERS COMP. & TECH. L.J. 77 (2008) (categorizing types of government hacking); Rachel S. Martin, Note, *Watch What You Type*, 40 AM. CRIM. L. REV. 1271 (2003) (arguing that keystroke monitoring should require a super-warrant); Angela Murphy, Note, *Cracking the Code to Privacy*, 1 DUKE L. & TECH. REV. 1 (2002) (explaining the *Scarfo* case).

<sup>12</sup> This article is focused exclusively on government hacking for law enforcement purposes. Hacking for national security purposes introduces further legal complications

The balance of the piece is organized in three parts. Part I conceptualizes possible sources of Fourth Amendment protection when the government deploys malware. In one view, the Constitution safeguards electronic devices against government intrusion; another perspective is that Fourth Amendment analysis should proceed from the data that investigators obtain. Government malware, in its most common configuration, places these two conceptions of constitutional privacy in direct conflict. I argue that recent Supreme Court guidance indicates these sources of protection are cumulative, not mutually exclusive, and courts must apply them in a two-step sequence.

Part II applies this two-step analysis to government malware. I conclude that installing malware will almost always constitute a search, requiring a warrant. I also conclude that the continuing operation of malware constitutes an ongoing search, requiring a continuously valid warrant. While the government need not provide *ex ante* notice of hacking, I explain why *ex post* notice is mandatory. Finally, in certain malware configurations, I note that the government must obtain a Wiretap Act “super-warrant.”

The Conclusion takes a normative step back. I argue that heightened constitutional and statutory safeguards, long applied to government wiretapping, should also apply to government hacking. The very same policy concerns that motivated checks on government wiretapping in the 1960s should motivate checks on government hacking today.

#### I. DOES THE FOURTH AMENDMENT PROTECT DEVICES OR DATA?

Fourth Amendment doctrine has long reflected two alternative conceptions of privacy. In one line of cases, rooted in English common law, the Constitution safeguards the integrity of personal spaces.<sup>13</sup> A government

---

(under the Fourth Amendment and the Foreign Intelligence Surveillance Act), as well as numerous additional policy dimensions. The article is also exclusively focused on hacking domestic computer systems. The extraterritorial scope of the Fourth Amendment remains a subject of professional and scholarly debate. *See generally* United States v. Ulbricht, No. 14-cr-68 (KBF), 2014 U.S. Dist. LEXIS 145553, at \*13-15 (S.D.N.Y. Oct. 10, 2014) (considering how the Fourth Amendment might apply to the search of a foreign server); Jennifer C. Daskal, *The Un-Territoriality of Data*, \_\_ YALE L.J. \_\_ (2016) (arguing that traditional Fourth Amendment concepts of territoriality are a poor fit for electronic data); David G. Delaney, *Widening the Aperture on Fourth Amendment Interests*, 68 STAN. L. REV. ONLINE 9 (2015) (similar); Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285 (2015) (summarizing territorial Fourth Amendment doctrine and applying it to international data searches). Since the most common deployment of government malware appears to be for identifying a computer system, and since there is a significant chance that a hacked system will be inside the United States, it is understandable that the common government practice is to prophylactically obtain a warrant.

<sup>13</sup> *See* Entick v. Carrington, 19 Howell’s St Trials 1029 (CP 1765) (establishing government liability for trespasses to real and personal property).

intrusion into a zone of privacy—physical or virtual—engages the Fourth Amendment’s procedural protections.

A second line of cases, tracing to the seminal 1967 opinion in *Katz v. United States*, emphasizes the information that investigators obtain.<sup>14</sup> Courts have exempted certain categories of data from the Fourth Amendment’s scope, and have crafted heightened protections for certain other categories of data.

Government hacking often places these two conceptions of privacy, and these two lines of cases, in tension—each suggesting an opposite result. This Part sketches the two Fourth Amendment perspectives, motivated by a simplified (but accurate) model of the most common law enforcement malware.<sup>15</sup>

Imagine that a criminal, Mallory, has hidden her identity behind anonymizing software.<sup>16</sup> Mallory is on a nameless financial fraud spree across the Internet; FBI agents are determined to unmask and prosecute her.<sup>17</sup>

In order to identify Mallory, the FBI agents propose to deploy malware that will circumvent her anonymizing software. It operates in two steps.

1. The law enforcement malware surreptitiously exploits a security flaw in Mallory’s computer, granting it the capability to examine her system configuration, read her files, and otherwise execute arbitrary code.
2. The malware periodically gathers the Internet Protocol address assigned to Mallory’s network by her Internet service provider, and it reports this information back to the FBI.

After the malware is successfully deployed, the FBI agents will serve a grand

---

<sup>14</sup> 389 U.S. 347 (1967) (holding that the Fourth Amendment protects private, real-time communications).

<sup>15</sup> See Email From Philippe Vinci Re: Meeting in Quantico (May 5, 2015), available at <https://wikileaks.org/hackingteam/emails/emailid/2821> (Leaked email from a malware vendor relaying a conversation with FBI officials. “In the past their targets were 20% on TOR, now they are 60% on TOR. They want to be able to catch the IP of their targets using TOR.”).

<sup>16</sup> The character Mallory is borrowed from computer security research literature, where she commonly denotes a malicious actor.

<sup>17</sup> In this hypothetical, and throughout the piece, I focus on FBI hacking. Public disclosures have emphasized the FBI, and all the hacking warrants that I encountered involved an FBI affiant. The Drug Enforcement Administration (DEA) has, though, confirmed that it also possesses and uses malware. See Letter from Assistant Attorney General Peter J. Kadzik to Senator Charles E. Grassley (July 14, 2015), available at <https://s3.amazonaws.com/s3.documentcloud.org/documents/2167965/doj-dea-letter-to-sen-grassley-re-hacking-team.pdf> (explaining that the DEA used a particular commercial hacking tool 17 times in a foreign country, pursuant to foreign court orders).

jury subpoena on Mallory's Internet service provider to verify her identity. They will then continue their investigation using conventional techniques.

Subpart A articulates a device-centric theory of the Fourth Amendment, emphasizing the integrity of Mallory's computer. From this perspective, focusing on step 1, the FBI agents would be conducting a constitutional search. They must usually obtain a warrant.

Subpart B sets out a data-centric conception of the Fourth Amendment, focusing on step 2 and the information that investigators obtain. This latter view suggests that the agents would not conduct a search, and need not obtain a warrant.

Subpart C then evaluates alternatives for reconciling these competing viewpoints, drawing on the Supreme Court's most recent Fourth Amendment guidance. The best interpretation of doctrine, I conclude, is that these two perspectives are cumulative.

### A. A Device-Centric Theory

Since the 19th century, the Fourth Amendment's procedural safeguards have unambiguously applied to closed containers.<sup>18</sup> Most modern opinions frame this protection in the familiar language of the *Katz* analysis. A person has a "reasonable expectation of privacy" in the contents of a sealed package, such that a government intrusion constitutes a Fourth Amendment search.<sup>19</sup>

Some opinions have also emphasized property rights, especially following the Supreme Court's recent reinvigoration of Fourth Amendment trespass doctrine.<sup>20</sup> Merely touching a closed container, for the purpose of obtaining information, could be sufficient to trigger Fourth Amendment search protections.<sup>21</sup>

---

<sup>18</sup> *Ex Parte Jackson*, 96 U.S. 727, 735 (1877) ("[R]egulations . . . cannot be enforced in a way which would require or permit an examination into . . . sealed packages . . . without warrant, issued upon oath or affirmation, in the search for prohibited matter . . .").

<sup>19</sup> *E.g.*, *United States v. Chadwick*, 433 U.S. 1, 11 (1977) ("By placing personal effects inside a double-locked footlocker, respondents manifested an expectation that the contents would remain free from public examination.").

<sup>20</sup> *See Florida v. Jardines*, 133 S. Ct. 1409, 1414-17 (2013) (following *Jones* and applying it to a drug-sniffing dog on residential curtilage); *United States v. Jones*, 132 S. Ct. 945, 949-53 (2012) (noting a property-based conception of the Fourth Amendment, and applying it to attachment of a GPS tracking device). Whether this trespass test applies to purely electronic searches remains ambiguous. *United States v. Jones*, 132 S. Ct. 945, 962-53 (2012) (Alito, J., concurring in the judgment) ("[T]he Court's reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact . . .").

<sup>21</sup> *E.g.*, *United States v. Thomas*, 726 F.3d 1086, 1092-93 (9th Cir. 2013). Similarly, manipulating or retaining a container could constitute sufficient interference with possessory interests to trigger Fourth Amendment seizure protections. *E.g.*, *State v. Kelly*, 708 P.2d 820,

Courts have consistently extended these closed-container protections to information technology devices, often reasoning by analogy. A computer, the thinking goes, is somewhat like an electronic (and exceptionally capacious) filing cabinet.<sup>22</sup> The analogy has its shortcomings, to be sure; courts have imposed limits on procedural protections for closed containers, including where a container is searched incident to arrest,<sup>23</sup> in an automobile,<sup>24</sup> or in plain view.<sup>25</sup> The extraordinary sensitivity and volume of computer data suggests that those container search caveats should be narrower when applied to electronic devices, if they apply at all. But in the first instance, when determining whether a search (or seizure) has taken place, the closed-container analogy has continuing value and vitality.

Applying this device-centric perspective to the government hacking hypothetical is quite straightforward. When the FBI agents break into Mallory's computer, they will be functionally cracking open a closed container. That breach of device integrity constitutes a Fourth Amendment search; barring exigent circumstances, they must first obtain a warrant.<sup>26</sup>

### B. A Data-Centric Theory

In *Katz*, the Supreme Court announced a branch of doctrine that emphasizes the information that the government obtains. “[T]he Fourth Amendment protects people, not places,” the Court memorably explained.<sup>27</sup> *Katz* itself dealt with a positive expansion of constitutional privacy protection; intercepting real-time communications content, the Court held, implicates the Fourth Amendment.

---

823-24 (Haw. 1985).

<sup>22</sup> See, e.g., *United States v. Andrus*, 483 F.3d 711, 718-19 (10th Cir. 2007) (assessing appropriate Fourth Amendment analogies for computer systems, and concluding that “it seems natural that computers should fall into the same category as suitcases, footlockers, or other personal items that command[] a high degree of privacy” (citation omitted)).

<sup>23</sup> See *Riley v. California*, 134 S. Ct. 2473, 2488-95 (2014) (holding that search incident to arrest doctrine does not apply to electronic devices).

<sup>24</sup> See *United States v. Burgess*, 576 F.3d 1078, 1087-90 (10th Cir. 2009) (discussing whether the the automobile search exception to the warrant requirement should apply to computers); *Wertz v. Indiana*, No. 48A04-1409-CR-427, at 6-11 (Ind. Ct. App. July 7, 2015) (holding that the automobile search exception does not apply to electronic devices).

<sup>25</sup> See *United States v. Carey*, 172 F.3d 1268, 1272-74 (10th Cir. 1999) (noting the challenge of applying plain view doctrine to computer searches).

<sup>26</sup> See *California v. Acevedo*, 500 U.S. 565, 580 (1991) (“It remains a ‘cardinal principle that searches conducted outside the judicial process . . . are *per se* unreasonable under the Fourth Amendment . . . .” (citing *Katz v. United States*, 389 U.S. 347, 357 (1967))); *United States v. Katzin*, 732 F.3d 187, 197-205 (3d Cir. 2013) (noting and applying the view that once a law enforcement practice is categorized as a Fourth Amendment search, it usually requires a warrant).

<sup>27</sup> *Katz v. United States*, 389 U.S. 347, 351 (1967).

Subsequent opinions that have invoked the *Katz* test, though, have tended to apply it in a negative manner. Where a piece of information has not been kept *entirely* secret from third-party businesses or public vantage points, courts have generally declined to recognize constitutional privacy safeguards.<sup>28</sup> Courts have held that there is categorically no reasonable expectation of privacy—and therefore no Fourth Amendment protection—in subscriber information,<sup>29</sup> communications metadata,<sup>30</sup> and geolocation records.<sup>31</sup> Congress has acted in accord with these views, developing a (notoriously complex) statutory scheme that generally allows for warrantless law enforcement access to these types of data.<sup>32</sup>

Applying this data-centric theory to government malware requires carefully parsing the information that law enforcement will obtain. Were investigators to collect real-time communications content, for instance, *Katz*'s sibling case *Berger v. New York* and its implementation in the Wiretap Act would mandate heightened “super-warrant” procedures.<sup>33</sup>

In the hypothetical above, however, the FBI agents propose to solely obtain non-content network configuration information. A data-centric conception of the Fourth Amendment would recognize that this category of record is exempt from constitutional privacy safeguards; the agents are not proposing a search, and they need not obtain a warrant.<sup>34</sup>

---

<sup>28</sup> Courts and commentators have developed a range of terms for describing these doctrines, including the “third-party doctrine,” “metadata doctrine,” and “public movements doctrine.” Whatever the terminology, the underlying rationales are shared.

<sup>29</sup> *See, e.g.*, *United States v. Perrine*, 518 F.3d 1196, 1204-05 (10th Cir. 2008) (holding that communications subscriber information is not protected by the Fourth Amendment and collecting similar cases).

<sup>30</sup> *See, e.g.*, *United States v. Forrester*, 512 F.3d 500, 509-11 (9th Cir. 2007) (concluding that surveillance of communications non-content, i.e. metadata, does not implicate the Fourth Amendment).

<sup>31</sup> *See, e.g.*, *United States v. Davis*, 785 F.3d 498, 505-18 (11th Cir. 2015) (holding that the third-party doctrine precludes Fourth Amendment protection for cell site location records); *In re Application of the United States for Historical Cell Site Data*, 724 F.3d 600, 608-15 (5th Cir. 2013) (same). *But see, e.g.*, *Tracey v. State*, 152 So. 3d 504, 511-26 (Fla. 2014) (reaching the opposite conclusion).

<sup>32</sup> *See* 18 U.S.C. § 2703(c)(2) (authorizing law enforcement access to subscriber records and telephone metadata with a grand jury or administrative subpoena); § 2709 (granting national security letter administrative subpoena authority for subscriber records and telephone metadata); § 2703(d) (establishing an intermediate court order for non-content records, including Internet communications metadata and device geolocation).

<sup>33</sup> 388 U.S. 41, 54-60 (1967) (invalidating the New York wiretapping statute and suggesting heightened Fourth Amendment requirements for wiretapping); 18 U.S.C. § 2518 (establishing procedural protections for real-time content interception beyond the conventional warrant requirements of probable cause and particularity). In criminal procedure discourse, special orders under the Wiretap Act are often dubbed “super-warrants.”

<sup>34</sup> As a purely statutory matter, the agents would require a “pen/trap” court order that

### C. Reconciling the Two Theories

To recap: in the most common law enforcement malware scenario, these two theories of Fourth Amendment protection arrive at contradictory conclusions. Plainly a doctrinal reconciliation is necessary.

As a matter of logic, there are four apparent options. One of the two doctrines might form the sole basis for malware jurisprudence, ignoring the other. Alternatively, courts might adopt the lesser or greater protections between the two theories. The following table outlines these four options, and the Fourth Amendment procedures that would result.<sup>35</sup>

	<b>Non-Content Communications Data</b>	<b>Real-Time Communications Content Data</b>
<b>Solely Device-Centric</b>	Warrant Required	Warrant Required
<b>Solely Data-Centric</b>	No Warrant Required	Super-Warrant Required
<b>Lesser Protection</b>	No Warrant Required	Warrant Required
<b>Greater Protection</b>	Warrant Required	Super-Warrant Required

The balance of this Subpart addresses each of these alternatives. I quickly dispense of the solely device-centric and lesser protection options, owing to unacceptable consequences. I then give a more detailed treatment for the remaining two possible doctrinal outcomes.

#### 1. Solely the Device-Centric Theory

Deferring exclusively to the device-centric theory cannot be correct, owing to how it addresses real-time interception of communications content. A simple hypothetical demonstrates the shortcoming.

Imagine that the FBI agents sought to tamper with a voice-over-IP

---

authorizes metadata surveillance (i.e. a pen register and trap and trace device). 18 U.S.C. §§ 3121-23. This type of order does not involve any sort of substantive judicial scrutiny, though; it “shall” issue once investigators self-certify relevance to an investigation.

<sup>35</sup> I do not include stored, non-communications data in the table for two reasons. First, that information will generally have been kept secret on a person’s device, mooted the applicability of the data-centric theory. (That assumption is quickly changing, though—many devices now perform routine data backups, including Apple’s popular iPhones and iPads.) Second, constitutional doctrine for stored content that is not entirely secret (i.e. is stored with a cloud service) has converged on a warrant requirement. *See United States v. Warshak*, 631 F. 3d 266 (6th Cir. 2010) (finding a reasonable expectation of privacy in stored email). Large technology firms now refuse to disclose stored content without a warrant, and law enforcement agencies have declined to litigate the issue. There is, consequently, no difference between the two theories for stored content on an electronic device.



application on Mallory's computer, such that they could listen in on her phone calls. In a purely device-centric reconciliation, the agents would need to obtain a warrant—they propose to breach the integrity of Mallory's computer, a practice that constitutes a Fourth Amendment search. The constitutional analysis would end there.

That result would be a radical downward departure in the procedural protections that apply to intercepting a telephone conversation. In order to operate a conventional telephone wiretap, the agents would be required to obtain a super-warrant. What's more, the wiretap would be implemented on equipment controlled by Mallory's service provider, not by intruding into a device that Mallory herself owns.

The doctrine for government malware should not impose a *lesser* procedural burden for obtaining the *same* information in a *more* intrusive manner. Otherwise, law enforcement officers would have a perverse incentive to deploy malware as an end-run around longstanding wiretapping protections. Given the (desirable) motivation to zealously investigate offenses, and given the (less desirable) resource constraints imposed on law enforcement, what investigator would volunteer to fill out more paperwork, satisfy more exacting scrutiny, and rely upon the cooperation of a third-party business?

In more precise Fourth Amendment terminology, it would be an incongruous result if a telephone-based wiretap could be deemed "reasonable" only pursuant to a super-warrant, but a malware-based wiretap could be "reasonable" with just an ordinary warrant. This consequence indicates that a reconciliation relying solely on the device-centric theory cannot be correct.

## 2. The Lesser Protection of the Two Theories

This option suffers from the exact same shortcoming as adopting solely the device-centric theory, and it should be rejected on the exact same basis. Law enforcement officers would remain incentivized to resort to malware, rather than conventional wiretaps, and a more intrusive malware search would be "reasonable" with lesser safeguards.

What's more, there is essentially no precedential basis for selecting this reconciliation. When courts have acknowledged both device-centric and data-centric strands of jurisprudence, they have either chosen between the theories<sup>36</sup> or treated them as cumulative.<sup>37</sup> After an exhaustive search, there

---

<sup>36</sup> See, e.g., *United States v. Skinner*, 690 F.3d 772, 777-81 (6th Cir. 2012) (holding that police tracking using a mobile phone's built-in GPS does not implicate the phone's integrity, and is governed by the public movements doctrine).

<sup>37</sup> See, e.g., *Riley v. California*, 134 S. Ct. 2473, 2492-93 (2014) (recognizing that phone

does not appear to be a single opinion that acknowledges two distinct levels of Fourth Amendment protection as binding on a law enforcement practice, then expressly selects the lesser level of protection.

### 3. Solely the Data-Centric Theory

According to documents released under the Freedom of Information Act, FBI agents have historically favored deferring exclusively to the device-centric theory.<sup>38</sup> The warrant application in the Timberline investigation, in fact, expressly declined to concede that the government's hacking to obtain identifying information would constitute a search and necessitate a warrant.<sup>39</sup>

It is not apparent whether federal investigators have acted upon this lax interpretation of the Fourth Amendment. Guidance from the Department of Justice Computer Crime and Intellectual Property Section, dating back to a

---

call logs are not themselves constitutionally protected, but holding that government access to a mobile phone to obtain call logs constitutes a search).

<sup>38</sup> See Email from [Redacted] to [Redacted] Re: IPAV (May 11, 2006), *available at* <https://www.eff.org/document/fbicipav-3pdf> ("I think that you most likely were told that a simple IPAV would be used initially, in which case I would agree with your initial analysis. [Redacted, apparent description of additional hacking steps to provide contrast.] This clearly requires a search and therefore a warrant and/or consent."); Email from [Redacted] to [Redacted] Re: [Redacted] (Aug. 24, 2005), *available at* <https://www.eff.org/document/fbicipav-14pdf> ("I still think that use of [redacted] is consensual monitoring without need for process . . . . That said, I will try to contort my mind into a different position if you still think otherwise."); Email from [Redacted] to [Redacted] (Aug. 23, 2005), *available at* <https://www.eff.org/document/fbicipav-03pdf> (whether a search warrant is required "is a hotly debated issue, and as of yet there is no policy guidance issued"); Email from [Redacted] to [Redacted] Re: UCO Proposal (Dec. 8, 2004), *available at* <https://www.eff.org/document/fbicipav-01pdf> ("We all know that there are IPAVs and then there are IPAVs. Of course the technique can be used in a manner that would require a court order. We need to know how/when to draw the line for obvious reasons."); Email from [Redacted] to [Redacted] Re: UCO Proposal (Dec. 8, 2004), *available at* <https://www.eff.org/document/fbicipav-01pdf> ("I don't necessarily think a search warrant is needed in all [hacking] cases . . . ."); Email from [Redacted] to [Redacted] Re: UCO Proposal (Dec. 1, 2004), *available at* <https://www.eff.org/document/fbicipav-01pdf> ("the safest course is to secure a warrant, though one might arguably not be required"); Email from [Redacted] to [Redacted] Re: IPAVs (Aug. 4, 2004), *available at* <https://www.eff.org/document/fbicipav-01pdf> ("There is an argument that at least the simplest IPAV is essentially akin to a [redacted] command and that under this principle may be used without a court order.").

<sup>39</sup> Application and Affidavit of FBI Special Agent Norman B. Sanders for a Computer and Internet Protocol Address Verifier Warrant, No. MJ07-5114, at 2 n.2 (W.D. Wash. June 12, 2007) ("In submitting this request, the Government respectfully does not concede that . . . a reasonable expectation of privacy is abridged by the use of this communication technique, or that the use of this technique to collect a computer's IP address, MAC address or other variables that are broadcast by the computer whenever it is connected to the Internet, constitutes a search or seizure.").

2002 memorandum, has consistently recommended a search warrant at minimum.<sup>40</sup> FBI investigators have emphasized that the agency is not bound by that conclusion,<sup>41</sup> though, and one email hints at past instances of hacking without first obtaining a warrant.<sup>42</sup>

The law enforcement inclination toward a solely data-centric Fourth Amendment theory is understandable. In the most common configuration of government malware, officers could begin deployment without the roadblocks of developing and demonstrating probable cause.

There is, furthermore, a colorable case law foundation for this theory. In several scenarios involving modern investigative technology, courts have conducted a Fourth Amendment analysis that emphasizes the information that law enforcement obtains—rather than how it obtains it.

This subpart attempts to articulate the best precedential basis for the FBI's preferred doctrinal reconciliation, drawing on opinions that assess mobile phone location tracking, surveillance by Internet service providers, and police inspection of mobile phone serial numbers. I then evaluate the weight of support, concluding that the favorable cases are questionable as precedent and distinguishable on critical facts.

#### a. Mobile Phone Location Tracking

One line of relevant cases arises from mobile phone location tracking. Some courts have reasoned that, because police officers could track a suspect's public movements without triggering Fourth Amendment safeguards (i.e. by tailing), they may electronically obtain the suspect's movements without procuring a warrant.<sup>43</sup>

Opinions that address “pinging” mobile phones or activating built-in GPS functionality have placed particular reliance on this reasoning.<sup>44</sup> The usual

---

<sup>40</sup> See Email from [Redacted] to [Redacted] Re: UCO Proposal (Dec. 1, 2004), *available at* <https://www.eff.org/document/fbicipav-01pdf> (“According to guidance issued by DOJ CCIPS, DOJ has ‘consistently advised AUSAs and agnets [sic] proposing to use IPAVs to obtain a warrant to avoid the exclusion of evidence.’ This opinion is dated March 7, 2002, written by [redacted].”).

<sup>41</sup> See Email from [Redacted] to [Redacted] Re: UCO Proposal (Dec. 8, 2004), *available at* <https://www.eff.org/document/fbicipav-01pdf> (“[I]t is my understanding that there is a disagreement on the status of the IPAV between what FBI/OGC says and what DOJ/CCIPS [sic]. If OGC will set out a policy on this, we will be glad to rely on it.”).

<sup>42</sup> See Email from [Redacted] to [Redacted] Re: IPAV/CIPAV (Nov. 22, 2004), *available at* <https://www.eff.org/document/fbicipav-01pdf> (“He wants all [special agents] to know that [the Office of the General Counsel] expects a [search warrant] for all IPAV/CIPAV applications (no getting around [the Operational Technology Division] by going to another Division that currently doesn't follow CCIPS guidance on this point).”).

<sup>43</sup> See, e.g., *United States v. Forest*, 355 F.3d 942, 951 (6th Cir. 2004).

<sup>44</sup> Courts have not been precise in describing the government practice of “pinging”

justification for exempting mobile phone location data from Fourth Amendment protection is that it constitutes a routine business record, knowingly disclosed to a third party (i.e. the suspect's phone company).<sup>45</sup> That rationale is strained when the government affirmatively causes the suspect's device to generate incriminating location data.<sup>46</sup> Courts have, consequently, resorted to data-centric analogies.

A pair of Sixth Circuit opinions exemplify the line of argument. In a 2004 ruling, a three-judge panel concluded that government generated mobile phone location data is "simply a proxy" for a police tail, and does not implicate the Fourth Amendment.<sup>47</sup> Another panel reaffirmed that holding in 2012, elaborating that "[u]sing a more efficient means of discovering [the same public location] information does not amount to a Fourth Amendment violation."<sup>48</sup> It bolstered its conclusion with the observation that "[I]aw enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system."<sup>49</sup>

A parallel argument can easily be constructed for law enforcement malware. The government's hacking, the reasoning goes, is "simply a proxy" for subpoenaing unprotected network configuration information. "Using a more efficient means of discovering [the same network configuration] information does not amount to a Fourth Amendment violation." And to hold

---

mobile phones. Some opinions appear to reference collection of solely cell tower data, as distinct from GPS data. *E.g.*, *United States v. Skinner*, 690 F.3d 772, 787 (6th Cir. 2012) (suggesting "ping" data is distinct from GPS data). Other opinions deploy the term to describe both GPS-based and tower-based location. *E.g.*, *United States v. Caraballo*, 963 F. Supp. 2d 341, 346 (D. Vt. 2013) ("This investigative technique, commonly referred to as cell phone 'pinging,' consists of the cell phone carrier surreptitiously accessing by satellite the cell phone's GPS location, or if unavailable, its location in terms of its proximity to the nearest cell phone tower.").

<sup>45</sup> *See, e.g.*, *United States v. Davis*, 785 F.3d 498, 505-18 (11th Cir. 2015) (concluding that routine cell site location data is a type of third-party business record, outside the scope of Fourth Amendment protection).

<sup>46</sup> The third-party doctrine rationale is even further strained when the government collects location data directly, such as with a "cell site simulator" device (commonly called an "IMSI catcher" or "Stingray"). *See* Brian L. Owsley, *TriggerFish, StingRays, and Fourth Amendment Fishing Expeditions*, 66 *Hastings L.J.* 183 (2014) (explaining cell site simulator technology and surveying District Court opinions). Given the relative paucity of case law on cell site simulators—to date, not one federal appellate court has rigorously reviewed the technology—the discussion above emphasizes other mobile phone tracking techniques.

<sup>47</sup> *United States v. Forest*, 355 F.3d 942, 951 (6th Cir. 2004).

<sup>48</sup> *United States v. Skinner*, 690 F.3d 772, 779 (6th Cir. 2012).

<sup>49</sup> *Id.* at 778. While I have many reservations about the *Skinner* opinion, I find this part particularly objectionable, since it has the law backward. Making a privacy-protecting choice *increases* a person's Fourth Amendment protection (i.e. reasonable expectation of privacy). Electing to have a conversation indoors, for instance, results in higher privacy safeguards than holding the chat in public.

otherwise would allow criminals to “circumvent[] the justice system,” rewarding them with heightened constitutional protections when they adopt anonymization software.

b. Internet Service Provider (ISP) Surveillance

Another developed line of cases involves Internet surveillance. In order to monitor a suspect’s web browsing and email metadata, investigators usually rely upon a “pen/trap” order, with substantially lesser protections than a search warrant.<sup>50</sup> Law enforcement officers serve the order on the suspect’s Internet service provider (e.g. Comcast). They then configure a filtering device on the ISP’s network, which sifts through the suspect’s traffic flows, extracts email metadata, and sends back the results.

Applying a data-centric theory of the Fourth Amendment to this fact pattern is challenging. In one perspective, the suspect’s web and email metadata is categorically unprotected, so law enforcement officers may obtain it without a warrant. In another perspective, though, the suspect’s ISP has no legitimate reason for peering into a customer’s network traffic. From the ISP’s vantage, a suspect’s web and email metadata could be considered communications content, since it plays no part in routing traffic.<sup>51</sup> When ISPs have previously conducted “deep packet inspection” on web metadata, in fact, they’ve been subjected to widespread consumer privacy criticism.<sup>52</sup>

Lower court opinions on ISP-based metadata surveillance have uniformly adopted the former perspective, holding that the practice is exempt from Fourth Amendment protection.<sup>53</sup> Judicial analysis has emphasized that metadata—whether phone, web, or email—is knowingly conveyed to *some* third parties. That fact alone is the beginning—and usually the end—of constitutional scrutiny.

The solely data-centric reconciliation for government malware doctrine certainly draws support from these cases. The underlying principle seems to

---

<sup>50</sup> When seeking prospective email metadata, law enforcement officers much more commonly serve a pen/trap order on the suspect’s email service (e.g. Google) and receive a real-time feed in response. Since this form of email surveillance does not implicate device integrity considerations, I focus solely on ISP-based email surveillance.

<sup>51</sup> An ISP need only examine IP addresses (and, sometimes, domain names) to provide Internet service to a subscriber. What’s more, web and email metadata are increasingly encrypted, such that an ISP cannot examine them.

<sup>52</sup> See, e.g., Peter Whoriskey, *Internet Provider Halts Plan to Track, Sell Users’ Surfing Data*, WASH. POST (June 25, 3008).

<sup>53</sup> See *United States v. Forrester*, 512 F.3d 500, 509-11 (9th Cir. 2007) (analyzing email and IP metadata); [Redacted], No. PR/TT [Redacted], at 58-62 (FISA Ct. 2004) (email metadata); *In re Application of the United States for an Order*, 396 F. Supp. 2d 45, 46- (D. Mass. 2005) (web and IP metadata); *United States v. Allen*, No. 99-0788 (C.A.A.F. 2000) (web metadata).

be that once a person has disclosed information to *some* third-party business, it loses all constitutional protection. Law enforcement can collect that information without triggering the Fourth Amendment's protections, even when they do not obtain the data directly from the intended third-party recipient.

c. Mobile Phone Serial Numbers

A third, very recent line of cases supports relying exclusively on the data-centric theory. When police seize a mobile phone, they must usually obtain a warrant to search the electronic contents.<sup>54</sup> On occasion, officers have removed the back of the phone in order to observe its serial numbers. Defendants respond by moving to suppress derivative evidence, arguing that opening the phone constitutes a Fourth Amendment search, and police must first obtain a warrant.

Courts have, so far, sided with law enforcement on this issue. Reported opinions conclude that a person does not have a reasonable expectation of privacy in their mobile phone serial numbers, noting that a serial number is non-content identifying information<sup>55</sup> and invoking doctrine that sustains police stop-and-identify practices.<sup>56</sup>

This reasoning is directly applicable to government malware. Returning to the Mallory hypothetical, FBI agents are merely proposing to collect non-content network identifying information from her computer. What they suggest is, in essence, the online equivalent of a stop-and-identify.

\* \* \*

While these three lines of cases lend some support to the FBI position, their import is loaded with caveats. All three bodies of jurisprudence are of questionable vitality, and all three are distinguishable as against the facts of malware.

Beginning with the mobile phone location cases—lower courts are concluding, with increasing frequency, that phone location is protected by the Fourth Amendment.<sup>57</sup> Furthermore, five justices have signaled that they are

---

<sup>54</sup> See *Riley v. California*, 134 S. Ct. 2473, 2480-95 (2014) (implicitly holding that police inspection of the electronic contents of a mobile phone constitutes a search, and declining to permit warrantless mobile phone searches incident to arrest).

<sup>55</sup> *State v. Green*, No. 49,741-KA, at 20-21 (La. Ct. App. Apr. 15, 2015) (“Serial numbers merely serve to identify a particular phone and they do not contain any information relative to the electronic data that is actually stored on the cell phone.”).

<sup>56</sup> *United States v. Green*, No. 09-10183-GAO, at 5-7 (D. Mass. Jan. 11, 2010).

<sup>57</sup> See, e.g., *United States v. Cooper*, No. 13-cr-00693-SI-1, at \*15-26 (N.D. Cal. 2015) (concluding that historical cell site location records can be protected by the Fourth

prepared to rule in favor of constitutional protection for phone location records.<sup>58</sup> Conventional wisdom among Court observers is that this line of cases will be sharply limited—if not eliminated—in the coming years.<sup>59</sup>

What's more, most mobile phone location cases are readily distinguishable on the facts. Those law enforcement practices generally do not constitute hacking, by any reasonable definition. Mobile phones are designed to facilitate location by carriers, for purposes of providing service, theft tracking, and directing emergency aid. The government is not delivering malware to phones, breaking into a user's private space. Rather, the government is taking advantage of existing and standard phone functionality that is accessible by the wireless carrier.

Turning to the ISP-based surveillance cases, courts have not yet reevaluated those rulings in light of recent Fourth Amendment jurisprudence. Since the landmark *United States v. Warshak* opinion in 2010, courts have consistently recognized constitutional privacy protection in communications content held by third-party businesses.<sup>60</sup> To date, no court has grappled with how *Warshak* applies to ISP-based surveillance.

The facts of the ISP-based surveillance cases are also highly distinguishable. In those scenarios, investigators obtained communications metadata from *some* third-party business. It wasn't the *specific* third party that the suspect had conveyed metadata to for processing, but it was still *a* third party. Government malware, by contrast does not involve collecting data from *any* third party. That's because the suspect has not disclosed identifiable data to any third party, in conjunction with their online activity. The very purpose is to collect data from the suspect's *own* electronic device.

Finally, the mobile phone serial number cases offer scant support. There are just a handful of reported opinions; the only federal appellate court to discuss the issue noted it as a difficult, open question.<sup>61</sup> What's more, the

---

Amendment, and collecting cases and state statutes).

<sup>58</sup> *United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring) (“I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on. I do not regard as dispositive the fact that the Government might obtain the fruits of GPS monitoring through lawful conventional surveillance techniques.”); *id.* at 964 (Alito, J., concurring in the judgment) (“I conclude that the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment.”).

<sup>59</sup> *See, e.g.*, Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 313 (2012) (“The concurring opinions in *Jones* raise the intriguing possibility that a five-justice majority of the Supreme Court is ready to endorse a new mosaic theory of Fourth Amendment protection.”).

<sup>60</sup> 631 F. 3d 266 (6th Cir. 2010) (concluding that the Fourth Amendment applies to content stored with a communications service provider).

<sup>61</sup> *United States v. Green*, 698 F.3d 48, 53 (1st Cir. 2012) (“The question . . . whether

intrusiveness of a serial number inspection is very limited, and most fact patterns can be justified as a search incident to arrest<sup>62</sup> or an inventory search.

In sum, the FBI's past perspective—that government malware should be regulated solely by a data-centric Fourth Amendment—is non-frivolous. There is a degree of case law support. But that support is exceedingly thin, both legally and factually. The substantially superior reconciliation, I argue in the next subpart, is treating the device-centric and data-centric theories as mutually reinforcing.

#### 4. The Greater Protection of the Two Theories

Constitutional rights are, ordinarily, analyzed in a cumulative fashion; the government's scrupulous recognition of one fundamental guarantee does not excuse transgression of another. A similar approach could easily be applied within the Fourth Amendment's protection against unreasonable searches. Investigators would have to comply with the procedures mandated by *both* the device-centric theory *and* the data-centric theory.

This subpart finds substantial support for a cumulative reconciliation among recent Supreme Court guidance. It then turns to normative considerations, noting that predictability and administrability favor a compound conception of the Fourth Amendment.

##### a. Recent Supreme Court Guidance

In three recent opinions, the Supreme Court has grappled with competing integrity and data conceptions of the Fourth Amendment. And, in all three cases, the Court has treated those two theories of privacy as cumulative.

*United States v. Jones* evaluated the constitutional protections associated with a GPS tracking device attached to a suspect's car.<sup>63</sup> A majority of the Court held that, regardless of whether there is a cognizable Fourth Amendment interest in a person's location (the data theory), physically trespassing against a car constitutes a search (the integrity theory).<sup>64</sup>

In *Florida v. Jardines* the Court assessed police use of drug-sniffing dogs on real property.<sup>65</sup> The majority extended *Jones*, reasoning that even if there were no Fourth Amendment protection against a dog sniff (data), stepping

---

the . . . retrieval of [the defendant's] IMSI number constituted a search . . . is not, in our view, an easy one.”)

<sup>62</sup> See *United States v. Rodriguez*, No. 11-205 (JRT/LIB), at 3-4 (D. Minn. Jan. 10, 2012) (concluding that police inspection of a mobile phone's FCC ID number was permissible as a physical search incident to arrest).

<sup>63</sup> 132 S. Ct. 945 (2012).

<sup>64</sup> *Id.* at 950-53.

<sup>65</sup> 133 S. Ct. 1409 (2013).



onto a porch to conduct a dog sniff is sufficient trespass to become a search (integrity).<sup>66</sup>

Most recently, *Riley v. California* considered police search of a mobile phone incident to a suspect's arrest.<sup>67</sup> Among other fallback arguments in that case, the United States suggested that officers should be able to examine a phone's call log without obtaining a warrant.<sup>68</sup> The Court unanimously rejected that position; accessing the phone was itself a search (integrity), regardless of the specific information that officers obtained (data).

These three cases are, to be sure, not conclusive for how the Fourth Amendment should apply to government malware. Each of the three fact patterns involves a *physical* breach of integrity—attaching a device to a car, stepping onto a porch, and tapping a phone screen. Government hacking, by contrast, involves solely an *electronic* intrusion. As four justices noted in *Jones*, the Court has yet to explicitly rule on how the Fourth Amendment applies in that scenario.<sup>69</sup>

That said, it would be an odd result if the Constitution treated physical integrity as cumulative with data privacy, but treated electronic integrity as mutually exclusive. The modern history of the Fourth Amendment is premised on recognition that privacy interests go beyond physical metes and bounds; *Katz* conclusively established that a property interest is not necessary for constitutional privacy protection. What's more, lower courts already consistently acknowledge the Fourth Amendment's applicability to purely virtual, information technology spaces.<sup>70</sup> And, to the extent *Riley* suggests a meaningful difference between the integrity of physical containers and electronic devices, it signals a *greater* protection for information technology.<sup>71</sup>

#### b. Normative Considerations

There are additional, normative reasons to favor a cumulative reconciliation of the device-centric and data-centric Fourth Amendment theories.

---

<sup>66</sup> *Id.* at 1414-18.

<sup>67</sup> 134 S. Ct. 2473 (2014).

<sup>68</sup> *Id.* at 2492-93.

<sup>69</sup> 132 S. Ct. at 962 (“[T]he Court’s reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked.”).

<sup>70</sup> *See, e.g.*, *United States v. Warshak*, 631 F. 3d 266, 287 (6th Cir. 2010) (analogizing privacy interests in purely electronic data stores to privacy interests in hotel rooms and apartments).

<sup>71</sup> 134 S. Ct. at 2489-91 (comparing electronic device searches to physical searches, and concluding that the former implicate substantially greater privacy interests).

Imposing an across-the-board warrant requirement for government malware avoids a foreseeable doctrinal morass about when, exactly, the Fourth Amendment kicks in.<sup>72</sup> The alternative would require courts to carefully divvy up a computer's (virtual) innards, holding various parts to be within or without the scope of constitutional privacy safeguards.<sup>73</sup>

A warrant mandate also increases uniformity and predictability for law enforcement agencies. Rather than haggling with attorneys and scrutinizing local case law, officers can get started right away with drafting affidavits.

Finally, in the context of government malware, a warrant requirement is not much of a hurdle to impose.<sup>74</sup> By the time investigators have singled out a target computer system or user, they should have ample factual basis to substantiate probable cause.<sup>75</sup>

\* \* \*

Relative to the alternatives, a cumulative reconciliation of the two Fourth Amendment theories is supported by a wealth of doctrine and normative considerations. Courts should explicitly adopt the cumulative approach when reviewing government hacking requests, ending unnecessarily lingering uncertainty.

The Fourth Amendment analysis that results is a straightforward two-step test. A court must ask, first, whether a proposed investigative technique impinges on the physical or virtual integrity of an electronic device. If it does, the practice constitutes a Fourth Amendment search, and will ordinarily require a warrant.

Next, the court must assess whether the government's technique involves accessing data that has been disclosed to third parties, but nevertheless remains constitutionally protected. Under prevailing lower court doctrine, if the government enters a suspect's cloud service account, that will constitute a search and usually necessitate a warrant.<sup>76</sup> And, following guidance from

---

<sup>72</sup> Cf. *United States v. Jones*, 132 S. Ct. 945, 953-54 (2012) (articulating a doctrinal preference against "thorny" Fourth Amendment search problems).

<sup>73</sup> Cf. *Riley v. California*, 134 S. Ct. 2473, 2493 (2014) (arguing against ambiguous line-drawing exercises for various parts of a device).

<sup>74</sup> See Email from [Redacted] to [Redacted] Re: UCO Proposal (Dec. 8, 2004), available at <https://www.eff.org/document/fbicipav-01pdf> ("Until a policy or directive is put in place, [the Data Intercept Technology Unit] has and will [sic] support any case that obtains a search warrant. Over the last six months it has not proven to be an obstacle to investigations.").

<sup>75</sup> See Paul Ohm, *Probably Probable Cause*, 94 MINN. L. REV. 1514, 1538-42 (2010) (arguing that probable cause develops early in online investigations).

<sup>76</sup> See *United States v. Warshak*, 631 F. 3d 266, 282-88 (6th Cir. 2010) (holding that private data stored with a cloud service is entitled to Fourth Amendment protection); *United States v. Bode*, No. ELH-12-158, 2013 WL 4501303, at \*51-54 (D. Md. Aug. 21, 2013) (collecting cases).

both the Supreme Court and Congress, if investigators intercept real-time communications content they must ordinarily obtain a Wiretap Act super-warrant.<sup>77</sup>

This two-part test facilitates analyzing the constitutional protections that regulate a range of government investigative practices. The following subpart applies the two-part test, noting special cases and concluding that current law enforcement practice is constitutional—except with respect to warrant timing.

## II. EVALUATING THE CONSTITUTIONALITY OF MALWARE

Having conceptualized how the Constitution regulates government hacking, this Part applies the two-step analysis to address unsolved Fourth Amendment malware puzzles.<sup>78</sup>

Subpart A assesses the conditions under which government access to a computer system becomes a search. When investigators probe a consumer device, they must ordinarily obtain a warrant.

Subpart B applies the Fourth Amendment's probable cause and particularity requirements to government hacking. Using the two-part test as a lens, I observe that these warrant elements must be satisfied for both the computer system that the government hacks and the data that it extracts. I also explain how algorithmic determinations of probable cause and particularity can be operationalized, allowing for mass hacking in a small subset of investigations. I find that most, but not all, government hacking practices have comported with these core Fourth Amendment requirements.

Subpart C evaluates whether government malware constitutes an ongoing search. I conclude that it does, and that it requires a continuously valid warrant. After evaluating and rejecting various government approaches to extending the warrant time limit imposed by the Federal Rules of Criminal Procedure, I recommend that DOJ seek an amendment.

Subpart D closes by noting the applicability of constitutional wiretapping doctrine. Where law enforcement malware is configured to intercept real-time communications, officers must unambiguously obtain a super-warrant.

---

<sup>77</sup> See *United States v. Councilman*, 418 F.3d 67, 69-85 (9th Cir. 2005) (applying the Wiretap Act to email interception); 18 U.S.C. §§ 2510-11, 2516 (establishing detailed super-warrant procedures for interception of real-time communications content).

<sup>78</sup> These are, to be sure, not the only legal questions posed by government malware. I do not address the question of warrant venue, since that is primarily a matter of statute and procedural rule, and since there is already a voluminous rulemaking record on the subject. See Proposed Amendments to the Federal Rules of Criminal Procedure, Regulations.gov, <http://www.regulations.gov/#!docketDetail;D=USC-RULES-CR-2014-0004> (last visited July 14, 2015).

A. *When does government access become a search?*

For decades, courts have struggled to define what constitutes “hacking” or “unauthorized access” into a computer system. Under the federal Computer Fraud and Abuse Act, and parallel state statutes, the judiciary and scholars have developed at least seven distinct substantive tests.<sup>79</sup> While computer trespass doctrine is not directly applicable to government malware, owing to explicit statutory exceptions for law enforcement investigations, it illuminates the depth of the Fourth Amendment challenge.<sup>80</sup>

Thankfully, law enforcement malware appears to be highly concentrated in a specific fact pattern: identifying anonymous users, like in the Mallory hypothetical. And applying the two-step test to that fact pattern is easy. From a device-centric perspective, law enforcement is unambiguously breaching the integrity of Mallory’s computer. Surreptitiously circumventing application security protections and executing unwanted software would satisfy any of the various computer trespass tests. From a data-centric perspective, the agents are collecting unprotected network configuration information. The greater protection of these two theories is a warrant requirement, and that’s what the FBI agents must follow.

This analysis generalizes beyond malware that solely identifies a computer. As a rule of thumb, government software that actively probes a consumer device will usually constitute a search. That’s because consumer devices, unlike business servers, are usually configured to be private.<sup>81</sup> Accessing content will almost always implicate a device’s integrity, triggering Fourth Amendment safeguards.

---

<sup>79</sup> See Jonathan Mayer, *Computer Crime in the Courts 17-35* (Mar. 2015) (unpublished manuscript) (synthesizing substantive standards for authorization to access a computer system or information).

<sup>80</sup> See, e.g., 18 U.S.C. § 1030(f) (“This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.”).

<sup>81</sup> When the government remotely probes a business server, much more difficult line-drawing questions can arise. While investigating an online black market, for instance, federal investigators may have engaged in borderline hacking conduct. See Nik Cubrilovic, *Analyzing the FBI’s Explanation of How They Located Silk Road*, NEW WEB ORDER (Sept. 7, 2014), <https://www.nikcub.com/posts/analyzing-fbi-explanation-silk-road/> (collecting and technically analyzing government filings associated with locating the black market server). Some remote investigative practices against business servers do remain easily identifiable as searches, such as entering a user’s cloud service account without their permission. See Letter from Deputy Assistant Attorney General David Bitkower to the Advisory Committee on the Federal Rules of Criminal Procedure, at 5 (Dec. 22, 2014) (offering a government hacking scenario where investigators cannot serve a Stored Communications Act warrant on a service provider, and so they log into the suspect’s account themselves).

There are exceptions to this rule, to be sure. Consumer devices can advertise information to the public, such as on a peer-to-peer file sharing network. When government software communicates with a consumer device under those circumstances, there plainly is neither a breach of integrity, nor collection of information that is constitutionally protected despite third-party access. Law enforcement may obtain data without first seeking a warrant.<sup>82</sup>

Critically, this exemption for advertised data only applies to information made available on *public* networks. If the police obtain advertised data by intruding into a private network—even an unprotected wireless network—they are conducting a search and must usually obtain a warrant.<sup>83</sup> Moreover, if officers conduct a real-time intercept of advertised data on a private network, they are operating a wiretap and must obtain a super-warrant.<sup>84</sup>

Another (possible) exception to malware constituting a search is when the government activates preexisting device functionality that is partially controlled by a third-party business. An example: as discussed earlier, wireless carriers have the capability to remotely enable location reporting from a subscriber's device.<sup>85</sup> This functionality is required on mobile phones, does not involve bypassing any security safeguards, does not include delivering proprietary government software, and does not require entering into any user storage area. On the other hand, this capability is reserved for extraordinary circumstances, assuredly runs counter to a device user's privacy expectations, and involves tampering with device configuration solely for the government's benefit.<sup>86</sup> In my view, reasonable minds can disagree on how to apply the two-step test in this scenario, and whether these facts should be considered a Fourth Amendment search—or even malware at all. Whatever the resolution, this much is certain: only a small subset of

---

<sup>82</sup> Courts have unanimously concluded that government investigators may explore public file-sharing services without triggering Fourth Amendment safeguards. *See* *United States v. Hill*, 750 F.3d 982, 986 (8th Cir. 2014); *United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009); *United States v. Ganoe*, 538 F.3d 1117, 1127 (9th Cir. 2008); *United States v. Perrine*, 518 F.3d 1196, 1205 (10th Cir. 2008); *United States v. Norman*, 448 F. App'x 895, 897 (11th Cir. 2011).

<sup>83</sup> *See* *United States v. Ahrndt*, No. 3:08-CR-00468-KI, 2013 WL 179326, at \*16-23 (D. Or. Jan. 17, 2013) (invalidating warrantless search of an unprotected wireless network). In some scenarios, the police may be able to obtain consent from a person with authorized access to the private network. *See* *United States v. Sawyer*, 786 F. Supp. 2d 1352, 1355-57 (N.D. Oh. 2011).

<sup>84</sup> *See* *Joffe v. Google*, 746 F.3d 920, 926-36 (9th Cir. 2013) (applying the Wiretap Act to real-time content interception from unprotected wireless networks).

<sup>85</sup> *See* FCC Wireless E911 Location Rule, 80 Fed. Reg. 11,806 (Mar. 4, 2015) (discussing location capabilities of mobile phones and setting new accuracy requirements).

<sup>86</sup> *Cf.* *Company v. United States*, 349 F.3d 1132 (9th Cir. 2003) (applying the Wiretap Act to remote FBI activation of a car's built-in microphone using theft tracking functionality).

device functionality is remotely available to third parties. These fact patterns are readily distinguishable from most configurations of government malware.

A third possible exception worth mentioning, since it has been raised by both FBI agents and the Advisory Committee on the Rules of Criminal Procedure, is deployment of malware against computer trespassers.<sup>87</sup> (In policy circles, this practice is often dubbed “hack back.”) Courts have held that intentional trespassers on real property may not be entitled to Fourth Amendment protection for their personal property.<sup>88</sup> Similarly, the Wiretap Act allows for warrantless surveillance of communications to or from a computer trespasser, so long as the owner of the attacked computer system consents.<sup>89</sup>

Courts should decline to recognize a trespasser exception for government malware. For starters, reliance on the physical trespass analogy is factually flawed. A hacker has in no way placed the entirety of their own device “into” the system that they are hacking. Rather, they have selectively sent data to (and received data from) a victim computer.

Furthermore, the physical trespass cases involve temporarily abandoned personal property.<sup>90</sup> And even in those fact patterns, courts have sometimes recognized Fourth Amendment protections.<sup>91</sup> A hacker has not, in any sense, abandoned the integrity or contents of his or her computer. With high probability, in fact, the computer remains at the hacker’s home or on his or her person.

A direct application of the *Katz* test also cuts against recognizing a trespasser exception. A hacker has not manifested a diminished expectation

---

<sup>87</sup> See Judicial Conference of the United States, Advisory Committee on the Rules of Criminal Procedure, Criminal Rules Meeting 10 (Apr. 7, 2014), available at <http://www.uscourts.gov/rules-policies/archives/meeting-minutes/advisory-committee-rules-criminal-procedure-april-2014>; Email from [Redacted] to [Redacted] RE: [Redacted] (July 2, 2007), available at <https://www.eff.org/document/fbicpav-08pdf> (“It is just not well settled in the law that we can rely on the trespasser exception to the search requirement.”).

<sup>88</sup> See Luke M. Milligan, Note, *The Fourth Amendment Rights of Trespassers*, 50 EMORY L.J. 1357, 1367-74 (summarizing the state of Fourth Amendment doctrine involving physical trespassers).

<sup>89</sup> See 18 U.S.C. § 2511(2)(i), 2511(20); Department of Justice, Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations 177-79 (2009), <http://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf> (explaining the computer trespasser exception to the Wiretap Act).

<sup>90</sup> If a person has a closed container under his or her immediate control, the Fourth Amendment unambiguously applies. See *Oliver v. United States*, 466 U.S. 170, 179 n.10 (1984) (noting that, even in an entirely public area, Fourth Amendment protection remains for “effects upon the person”).

<sup>91</sup> See, e.g., *State v. Mooney*, 588 A.2d 145, 152-61 (Conn. 1991) (concluding that a trespasser had a reasonable expectation of privacy in a sealed duffel bag and cardboard box that he had abandoned).

of privacy in his or her *own* computer, by breaking into *someone else's* computer. Using personal property in the commission of a crime does not, by itself, negate Fourth Amendment protection. (If the law were otherwise, the unbroken line of closed container cases would be erroneous.)

Finally, the Supreme Court's recent guidance in *Riley* disfavors a trespasser exception. Modern technology contains data of extraordinary volume, duration, pervasiveness, and sensitivity.<sup>92</sup> That recognition weighs heavily in favor of a warrant requirement. A trespasser exception would allow the government to "hack back" and obtain a wealth of information, much of it not immediately related to defending the computer system under attack.<sup>93</sup>

Assuming that courts reject a trespasser exception, the resulting rules are straightforward. With a victim's consent, investigators may intercept information sent to or received by a hacker,<sup>94</sup> and may monitor data advertised by the hacker on the victim's network.<sup>95</sup> But, the moment investigators break into the hacker's computer, they are conducting a search and must ordinarily obtain a warrant.<sup>96</sup>

#### *B. How do probable cause and particularity apply to government hacking?*

---

<sup>92</sup> See *Riley v. California*, 134 S. Ct. 2473, 2488-91 (2014) (discussing ways in which the search of a mobile phone is far more intrusive than a physical search).

<sup>93</sup> A narrower trespasser exception, allowing the government solely to take steps to prevent an attack or identify the perpetrator, would mitigate this concern. But a narrower exception would have no doctrinal basis, and would require courts to rigorously parse and review each and every category of information that the government obtained.

<sup>94</sup> See 18 U.S.C. § 2511(2)(i) (allowing communications content interception against a computer trespasser, with a victim's consent).

<sup>95</sup> See *United States v. Stanley*, 753 F.3d 114, 119-24 (3d Cir. 2014) (holding that a network trespasser does not have a Fourth Amendment protection in his or her network configuration as exposed to the victim's network, but rejecting the argument that all information associated with the trespasser is exempt from protection).

<sup>96</sup> As with all Fourth Amendment searches, exigent circumstances may excuse the warrant requirement. The Supreme Court has noted that these are highly fact-specific determinations, and require extraordinary justification. See *Riley v. California*, 134 S. Ct. 2473, 2494 (2014) (listing bomb detonation and child abduction as hypothetical scenarios where a warrantless mobile phone search might be permissible). The rationale most likely to be applicable to computer trespassers is destruction of evidence, since most electronic attacks do not implicate human life or safety. See *Kentucky v. King*, 131 S. Ct. 1849, 1856-57 (2011) (noting various exigencies that excuse a search warrant). In order for that justification to apply, though, investigators must have reasonable grounds to believe that the hacker is destroying evidence in his or her own computer system. See *Ker v. California*, 374 U.S. 23, 57 (1963) (Brennan, J., concurring) ("Our decisions in related contexts have held that ambiguous conduct cannot form the basis for a belief of the officers that an escape or the destruction of evidence is being attempted."). While it is conceivable that some hackers will satisfy this standard—for instance, by issuing specific taunts—investigators will rarely have sufficient indicia that a hacker plans to purge data from his or her *own* computer.

The Fourth Amendment imposes two substantive constraints on a search warrant application: officers must demonstrate probable cause that they will find evidence of a crime, and they must describe that evidence with particularity. These two requirements are deeply intertwined; particularity scopes probable cause, linking it to a specific offense and type of evidence.

Courts are already struggling with how probable cause and particularity apply to information technology. Some courts have required *ex ante* search protocols, delineating particular pockets of stored data.<sup>97</sup> Others have allowed broad discretion for investigators, checked solely by *ex post* suppression motions.<sup>98</sup> (In my view, given the extraordinary qualities of data stored in electronic devices, and given the haziness of *ex post* suppression practice, *ex ante* restrictions are the better approach.) Law enforcement malware poses these same general problems, and introduces one more.

The government may not know *which* computer it is hacking. When deploying identification malware, the very purpose is to discover a computer's location and owner. The result is a seeming chicken-and-egg problem: how can investigators describe, with particularity, the very electronic device that they are attempting to discover?

The best solution, in my view, lies in the doctrine of "anticipatory" warrants.<sup>99</sup> Courts have long allowed for law enforcement searches and

---

<sup>97</sup> *See, e.g.*, In Re [Redacted]@gmail.com, 62 F. Supp. 3d 1100, 1102-04 (N.D. Cal.) (suggesting that, at minimum, the government must identify date restrictions and commit to returning or destroying relevant evidence in a cloud service search); In Re Search of Info. Associated with [Redacted]@mac.com, 25 F. Supp. 3d 1, 4-9 (D.D.C. 2014) (calling for online services to screen information made available to the government, according to specific times, keywords, parties, or other filtering criteria); United States v. Winn, No. 14-CR-30169-NJR, 2015 U.S. Dist. LEXIS 15240, at \*25-35 (S.D. Ill. Feb. 9, 2015) (invalidating a smartphone search warrant that covered "any or all files contained on said phone" as insufficiently particularized).

<sup>98</sup> *See, e.g.*, In re a Warrant for All Content & Other Info. Associated with the Email Account [Redacted]@gmail.com Maintained at Premises Controlled by Google, 33 F. Supp. 3d 386, 388-401 (S.D.N.Y. 2014) (holding that, in general, *ex ante* protocols for data searches are not required to satisfy the Fourth Amendment particularity standard).

<sup>99</sup> An anticipatory warrant rationale offers a comprehensive and coherent constitutional basis for identification malware. There are, to be sure, related lines of doctrine that could also be used to justify identification malware warrants. Courts have long permitted location tracking warrants; at the time of issuance, officers do not know where the suspect will travel. *See* United States v. Karo, 468 U.S. 705, 718 (1984) ("[I]t will still be possible to describe the object into which the beeper is to be placed, the circumstances that led agents to wish to install the beeper, and the length of time for which beeper surveillance is requested. In our view, this information will suffice to permit issuance of a warrant authorizing beeper installation and surveillance."). More recently, courts have allowed DNA-based "John Doe" arrest warrants; at the time of issuance, officers do not know the suspect's identity. *See* People v. Robinson, 224 P.3d 55, 71-76 (Cal. 2010).



arrests, subject to conditions that trigger execution.<sup>100</sup> The notion is that courts can, in advance, identify facts that are likely to occur—and that would satisfy probable cause and particularity once they do occur.<sup>101</sup> Investigators then wait for the specified triggering conditions and execute their warrant.

Cases involving controlled package delivery are the quintessential example.<sup>102</sup> Courts have consistently upheld search and arrest warrants conditioned upon receipt of a contraband parcel. In these scenarios, officers do not necessarily know, in advance, when the package will be accepted. Officers may not even know who will receive the package or where it will be delivered.<sup>103</sup> But it is likely that someone will accept the parcel, and accepting the parcel is a sufficient triggering condition to establish probable cause and particularity to both search the place of delivery and arrest the recipient.

Wiretaps are another established area of permissible anticipatory searches.<sup>104</sup> When seeking a “roving” super-warrant, investigators do not know in advance which places they will bug or which phone lines they will tap.<sup>105</sup> Courts have nevertheless sustained these investigatory practices, emphasizing that the touchstone of the Fourth Amendment is reasonable particularity—not exacting precision.<sup>106</sup>

---

<sup>100</sup> See *United States v. Grubbs*, 547 U.S. 90, 96 (2006) (“Anticipatory warrants are, therefore, no different in principle from ordinary warrants. They require the magistrate to determine (1) that it is *now* probable that (2) contraband, evidence of a crime, or a fugitive will be on the described premises (3) when the warrant is executed.”); *United States v. Garcia*, 882 F.2d 699, 701-04 (2d Cir. 1989) (reviewing the doctrine, policy, and precedent that support anticipatory warrants).

<sup>101</sup> See *Grubbs*, 547 U.S. at 96-97 (explaining that an anticipatory warrant requires probable cause both with respect to the triggering condition occurring and finding evidence once the triggering condition is satisfied). In a controlled delivery scenario, probable cause with respect to the triggering condition is easily satisfied—packages are usually delivered to their intended destination and recipient.

<sup>102</sup> See *id.* at 702-03 (collecting cases); Joshua D. Poyer, Note, *United States v. Miggins: A Survey of Anticipatory Search Warrants and the Need for Uniformity Among the Circuits*, 68 U. MIAMI L. REV. 701 (2004) (noting variations in exact requirements between circuits).

<sup>103</sup> In the usual controlled delivery fact pattern, investigators at least know the intended recipient and destination for a package. With a malware search, by contrast, officers cannot provide a name or address in advance. While that sort of *ex ante* ambiguity is rare in a controlled delivery, it has come up, and courts have sustained anticipatory warrants for unspecified addresses and individuals. See *People v. Duoc Boi*, 885 N.E.2d 506, 515-22 (Ill. App. Ct. 2008) (sustaining controlled delivery search warrant for “any other location” where a package is taken); *State v. Morris*, 668 P.2d 857 (Ala. Ct. App. 1983) (sustaining controlled delivery search warrant for “whoever picks up said package” and “wherever the described package is taken”).

<sup>104</sup> See *United States v. Grubbs*, 547 U.S. 90, 95-96 (2006) (noting that wiretap super-warrants are a type of anticipatory warrant).

<sup>105</sup> See 18 U.S.C. § 2518(11) (procedures for roving wiretaps and bugs).

<sup>106</sup> See, e.g., *United States v. Gaytan*, 74 F.3d 545, 553 (5th Cir. 1996) (following *Petti*); *United States v. Bianco*, 998 F.2d 1112, 1122-25 (2d Cir. 1993) (sustaining roving bug);

Government hacking follows the same principles as a controlled delivery or a roving wiretap. Agents may not know, in advance, the exact computer that they are breaching. But they can articulate a conditional set of facts to ensure a fair chance that their malware will be delivered, and when it is delivered, to a computer system that satisfies probable cause and particularity.

One possible malware trigger is affirmative conduct by a suspect. The FBI's "phishing" attack in the Timberline case is a good example. The target was actively using his social media account, so it was likely that an FBI message would be read. And, given the target's apparent ego, it was extra likely that he would click the FBI's bogus news link. Whoever first clicked that link was likely to be the person sending bomb threats, because they had demonstrated control over the social media account. And it was likely that their computer contained evidence of their crimes, i.e. identifying information. In more general terms: there was probable cause that the FBI's malware would be delivered to a computer, and there was probable cause that particular criminal evidence would be recovered from that particular computer.

This phishing approach is not foolproof, to be sure. The government must make sure it delivers malware to the right account; on at least one occasion, FBI agents have sent malware to the wrong email address.<sup>107</sup> Investigators must also take precautions to limit the likelihood of hacking innocent users; given that links can be trivially forwarded or indexed by a search engine, probable cause will quickly dissipate after a phishing attempt.<sup>108</sup> Restricting malware delivery to the first device to visit the phishing link, for instance, might be appropriate. But, in general, using phishing as an anticipatory warrant condition is a constitutionally sound investigative strategy.

Another possible anticipatory warrant approach is conditioning malware delivery on when the target visits a specific website. On at least two occasions, the FBI has seized an online service, then sent identification malware to *all* visitors.<sup>109</sup> This type of "watering hole" attack has proven

---

United States v. Petti, 973 F.2d 1441, 1443-45 (9th Cir. 1992) (sustaining roving wiretap). See also *Grubbs*, 547 U.S. at 97 ("The Fourth Amendment, however, does not set forth some general 'particularity requirement.' It specifies only two matters that must be 'particularly describ[ed]' in the warrant: 'the place to be searched' and 'the persons or things to be seized.').

<sup>107</sup> Second Amended Application and Third Amended Affidavit of FBI Task Force Officer William A. Gallegos for a Network Investigative Technique Warrant, No. 12-sw-05685-KMT (D. Colo. Dec. 11, 2013).

<sup>108</sup> See American Civil Liberties Union, on the Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media 22-23 (2014) (describing ways in which a government phishing attack could reach innocent parties).

<sup>109</sup> Application and Affidavit of FBI Special Agent Jeffrey Tarpinian for a Network

exceedingly controversial, since it can involve hacking thousands of users under just one search warrant.<sup>110</sup>

Using a watering hole trigger for government malware can, in my view, be constitutionally sustainable. Authorizing multiple searches under one warrant is no issue—courts have consistently permitted that practice.<sup>111</sup> A warrant under the Fourth Amendment requires valid judicial determinations, not formally formatted paperwork.<sup>112</sup>

The challenge is establishing probable cause of a crime, and describing evidence with particularity, based solely on a visit to a webpage. Making that determination is possible, but only in a *very* specific scenario—because the criminal statutes on child pornography are exceptionally broad, and because the speech protections for child pornography are exceptionally limited.

Possessing information, or attempting to possess information, is rarely itself a crime. And it constitutionally could not be a crime, owing to the First Amendment’s broad free speech protections. Child pornography is unique: possessing it or attempting to possess it *is* criminal, and the First Amendment allows for this broad criminalization.<sup>113</sup>

From a Fourth Amendment perspective, then: if a user visits a semi-private website that is exclusively dedicated to distributing child pornography, there is probable cause to believe that the user has committed a crime (attempted possession), and that the user’s computer contains particular evidence of that crime (identifying information). The FBI appears to rely upon this very reasoning in its watering hole deployments.<sup>114</sup>

---

Investigative Technique Warrant, No. 8:12MJ356, at 30 (D. Neb. Nov. 16, 2012) (“I request authority to use the NIT to investigate: (1) any user who accesses any page in the ‘Images’ section of ‘Bulletin Board A’ . . . .”); Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, WIRED (Sept. 13, 2013), <http://www.wired.com/2013/09/freedom-hosting-fbi/>. In a third watering hole deployment, discussed *infra*, malware delivery was conditioned on logging into the website.

<sup>110</sup> See American Civil Liberties Union, on the Proposed Amendment to Rule 41 Concerning “Remote Access” Searches of Electronic Storage Media 14-15 (2014) (criticizing government watering hole techniques).

<sup>111</sup> See 31 A.L.R.2d 864 (collecting cases that have permitted searches of multiple locations with a single warrant).

<sup>112</sup> See, e.g., *United States v. Rigmaiden*, No. CR 08-814-PHX-DGC, 2013 WL 1932800, at \*55-56 (D. Ariz. May 8, 2013) (explaining that a warrant need not use specific terminology, but rather, satisfy the Fourth Amendment’s basic requirements). As a matter of policy, greater clarity in warrant documentation is certainly preferable. That is not a constitutional requirement, though.

<sup>113</sup> 18 U.S.C. § 2251, 2252, 2252A; *United States v. Williams*, 533 U.S. 285, 292-304 (2008) (holding that an offer to provide or request to receive child pornography is categorically unprotected by the First Amendment); *New York v. Ferber*, 458 U.S. 747, 753-74 (1982) (holding that possession of child pornography is categorically unprotected by the First Amendment).

<sup>114</sup> See Application and Affidavit of FBI Special Agent Jeffrey Tarpinian for a Network

Most websites, though, serve multiple purposes and are open to the public. The government may need to impose extra conditions on its watering hole delivery—requiring more than merely visiting the site—to ensure probable cause. Waiting for a user to log in or send a private message, for instance, would offer a firmer footing. Prior watering hole warrants have involved both of these conditions.<sup>115</sup>

As with phishing, the government does not appear to have always correctly executed this strategy for developing probable cause. In a highly publicized episode, the FBI appears to have seized a set of web servers, then deployed malware to anyone visiting any of the hosted websites.<sup>116</sup> Some of those websites were dedicated to child pornography, such that probable cause may have existed for each visitor. But many of those websites hosted information that was not criminal, and that could not be criminal—rendering the FBI’s hacking of visitors constitutionally infirm.

*C. Does government malware require a continuously valid warrant?*

Under the two-step test, government hacking is almost always a search, and almost always requires a warrant. But when does the search occur? Is it solely at the moment of breaking into a device, or is it throughout the continued operation of the law enforcement malware? The answer to this dilemma is critical, since it dictates the necessary period of warrant validity.

The view of the Department of Justice appears to be that entering a computer system is generally a search, but remaining in a computer system is not. In the *Timberline* case, for instance, investigators combined a search warrant with a lesser pen/trap order. The search warrant was valid for 10 days, and covered installation and initial operation of the malware; the pen/trap order was valid for 60 days, and covered subsequent reports from the malware.<sup>117</sup>

Applying the two-step test, this procedural structure is inconsistent with

---

Investigative Technique Warrant, No. 8:12MJ356, at 30 (D. Neb. Nov. 16, 2012)

<sup>115</sup> Application and Affidavit of FBI Special Agent John Robertson for a Search Warrant, No. 1:15-mj-00534-VVP (E.D.N.Y. June 10, 2015) (describing a warrant that authorized malware delivery from a seized child pornography website “each time any user or administrator logged [in]”); Application and Affidavit of FBI Special Agent Jeffrey Tarpinian for a Network Investigative Technique Warrant, No. 8:12MJ356, at 30 (D. Neb. Nov. 16, 2012) (“I request authority to use the NIT to investigate: . . . (2) any user who sends or views a private message on ‘Bulleting Board A’ during the period of this authorization.”).

<sup>116</sup> Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, WIRED (Sept. 13, 2013), <http://www.wired.com/2013/09/freedom-hosting-fbi/>.

<sup>117</sup> Application and Affidavit of FBI Special Agent Norman B. Sanders for a Computer and Internet Protocol Address Verifier Warrant, No. MJ07-5114, at 13-14 (W.D. Wash. June 12, 2007).

the Fourth Amendment. Law enforcement hacking requires a warrant, at minimum, because it intrudes upon a device's integrity. That integrity remains compromised throughout the period that the government's malware is resident. There must, consequently, be a warrant with continuing validity for so long as the malware operates. A pen/trap order does not suffice, since it is not supported by probable cause.<sup>118</sup>

Drawing a parallel to physical searches is instructive. When the government compromises physical integrity to conduct a search, such as by installing a location tracker on a car<sup>119</sup> or an electronic device in a home,<sup>120</sup> courts have unhesitatingly concluded that an ongoing warrant is required. A rule allowing for continued malware operation without a warrant would represent a doctrinally unsubstantiated distinction between physical and electronic integrity.

Analogizing the data-centric theory of the Fourth Amendment also favors an ongoing warrant. The Supreme Court has emphasized that communications interception requires a continuously valid super-warrant, and the Wiretap Act imposes ongoing substantive requirements.<sup>121</sup> A rule permitting continued computer hacking with a one-time judicial determination would add unjustified inconsistency between the device-centric and data-centric conceptions of the Fourth Amendment.

The resulting temporal regulation of malware is straightforward. Under the current Federal Rule of Criminal Procedure 41, a warrant must be executed within 14 days of issuance. The government, then, has 14 days to hack a device and collect data from it. After 14 days, the government must either obtain a new warrant or disable its malware.<sup>122</sup>

---

<sup>118</sup> 18 U.S.C. § 3122 (requiring only a self-certification of relevance to substantiate a pen/trap order).

<sup>119</sup> *See, e.g.,* *United States v. Katzin*, 732 F.3d 187 (3d Cir. 2013) (“We thus have no hesitation in holding that the police must obtain a warrant prior to attaching a GPS device on a vehicle, thereby undertaking a search that the Supreme Court has compared to ‘a constable’s concealing himself in the target’s coach in order to track its movements.’” (citing *United States v. Jones*, 132 S. Ct. 945, 950 n.3 (2012))).

<sup>120</sup> *See, e.g.,* *Silverman v. United States*, 365 U.S. 505, 511-12 (1961) (“This Court has never held that a federal officer may without warrant and without consent physically entrench into a man’s office or home, there secretly observe or listen, and relate at the man’s subsequent criminal trial what was seen or heard.”).

<sup>121</sup> *Berger v. New York*, 388 U.S. 41, 59 (1967) (“[A]uthorization of eavesdropping for a two-month period is the equivalent of a series of intrusions, searches, and seizures . . . .”); 18 U.S.C. § 2518(5) (“No order entered under this section may authorize or approve the interception of any wire, oral, or electronic communication for any period longer than is necessary to achieve the objective of the authorization . . . .”).

<sup>122</sup> Courts have, in past, authorized deviation from Rule 41’s time limit for subsequent forensic examination of seized computer data. *See* *United States v. Kernell*, No. 3:08-CR-142, 2010 U.S. Dist. LEXIS 32845, at \*38-43 (E.D. Tenn. Mar. 31, 2010) (explaining the issue and collecting cases). That fact pattern is very different from government hacking, of

In at least three additional cases, the FBI has failed to adhere to this simple formulation. A 2012 warrant in the District of Colorado authorized malware operation for 14 days after installation (whenever that occurred), rather than 14 days after warrant issuance.<sup>123</sup> The accompanying affidavit suggested treating installation as a warrant triggering condition, allowing for extended time.<sup>124</sup> But that reasoning misunderstands the doctrine of anticipatory warrants, which allows for conditional search *execution*; the warrant is still *issued*, and the clock starts running, once it is signed by the reviewing judge.<sup>125</sup>

In a District of Nebraska investigation the same year, the FBI obtained a computer search warrant with two distinct time periods. Agents had 14 days to install malware delivery software onto a webserver that they had seized, in accordance with the Federal Rules.<sup>126</sup> But they then had 30 days to install and operate malware on computers that visited the website.<sup>127</sup> The warrant application did not justify this extended time limit, nor did it even indicate the source.

Most recently, a 2013 warrant application in the Southern District of Texas requested a 30-day period for installation and operation.<sup>128</sup> Once again, there was no asserted basis for the extended time limit. (In fact, the earlier Colorado affidavit expressly amended out a 30-day time limit, explaining that it was “mistaken.”<sup>129</sup>)

---

course—police have long been authorized to inspect evidence after seizure. *See id.* at \*38 (“The Court finds that the ten-day limitation on the execution of a search warrant applies to the initial seizure of the computer hardware.”); *United States v. Tillotson*, No. 2:08-CR-33, 2008 U.S. Dist. LEXIS 97741, at \*6 (E.D. Tenn. Dec. 2, 2008) (“The subsequent analysis of the computer’s contents is not a search in the sense contemplated by Rule 41 . . .”). And, at any rate, Rule 41 was explicitly amended to address the timing of post-seizure forensic examinations. FED R. CRIM. P. 41(e)(2)(B) (clarifying that the Rule 41 time limits apply to “the seizure or on-site copying of the media or information, and not to any later off-site copying or review”).

<sup>123</sup> Second Amended Application and Third Amended Affidavit of FBI Task Force Officer William A. Gallegos for a Network Investigative Technique Warrant, No. 12-sw-05685-KMT, at 23-24 (D. Colo. Dec. 11, 2013).

<sup>124</sup> *Id.* at 22.

<sup>125</sup> *See United States v. Grubbs*, 547 U.S. 90, 96 (2006) (explaining that an anticipatory warrant involves a present determination by a judge).

<sup>126</sup> Application and Affidavit of FBI Special Agent Jeffrey Tarpinian for a Network Investigative Technique Warrant, No. 8:12MJ356, at 34 (D. Neb. Nov. 16, 2012).

<sup>127</sup> *Id.* at 35.

<sup>128</sup> *In Re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 756 (S.D. Tex. 2013) (malware warrant application seeking “prospective data obtained during a 30-day monitoring period”).

<sup>129</sup> Second Amended Application and Third Amended Affidavit of FBI Task Force Officer William A. Gallegos for a Network Investigative Technique Warrant, No. 12-sw-05685-KMT, at 2-3 (D. Colo. Dec. 11, 2013).

Federal agents would, understandably, prefer not to be burdened with a malware warrant renewal every two weeks. Declassified FBI emails reflect extensive discussion about how to circumvent the explicit time limit imposed by the Federal Rules, including invocation of the (inapplicable) tracking device provisions of the Electronic Communications Privacy Act<sup>130</sup> and the (also inapplicable) All Writs Act.<sup>131</sup>

Rather than evade Rule 41 (and its constitutional basis) by invoking irrelevant statutes or slipping extra time into warrant applications, the government should propose a simple amendment. There is already a template: in order to facilitate location tracking devices, the Federal Rules were amended in 2006 with provisions that set out discrete time periods for installation and operation.<sup>132</sup> A similar set of time limits should be expressly

---

<sup>130</sup> See Email From [Redacted] to [Redacted] Re: 288A-SE-93709 (June 8, 2007), available at <https://www.eff.org/document/fbicipav-08pdf> (“The other three documents are ponies of an application for a mobile tracking order, a mobile tracking/PRTT order, and the affidavit supporting the two that ST. [sic] Louis drafted for a similar type order.”); Email From [Redacted] to [Redacted] Re: CIPAV Court Orders - As a Mobile Tracking Device 18 USC 3117 (Nov. 21, 2006), available at <https://www.eff.org/document/fbicipav-08pdf>. The tracking device statute, 18 U.S.C. § 3117, empowers courts to issue warrants for “tracking devices”; its implementation in Rule 41(e)(2)(C) specifies a maximum of 10 days for installation and 45 days for operation. The Department of Justice has consistently argued that these “tracking device” provisions do not cover purely electronic location techniques, in a bid to avoid a warrant requirement for mobile phone location tracking. See, e.g., In Re Application of the United States for an Order, 411 F. Supp. 2d 678, 681 (W.D. La. 2006). It would be incongruous for DOJ to reverse that critical argument, after a decade—and solely to extend a renewal clock in hacking cases. Moreover, identification malware does not itself locate a device in any conventional sense. Rather, it gives the government sufficient network and device configuration information to determine the owner’s identity through follow-up investigation.

<sup>131</sup> See Email From [Redacted] to [Redacted] Re: CIPAV Court Orders (Nov. 21, 2006), available at <https://www.eff.org/document/fbicipav-08pdf> (“One comment that has come in from my unit re the draft orders that should be forwarded to AUSA [redacted] is that he should also cite to the All Writs Act . . .”). Courts invoke the All Writs Act, 28 U.S.C. § 1651, to compel third-party assistance with warrant execution. That includes assistance with ongoing electronic surveillance. See *United States v. New York Tel. Co.*, 434 U.S. 159, 171-78 (1977) (sustaining use of a warrant, in conjunction with the All Writs Act, to compel a telephone company to prospectively provide call records). But the All Writs Act is only relevant to third-party assistance associated with an electronic search, not any ongoing nature of the search. See *United States v. Karo*, 468 U.S. 705, 711-21 (1984) (assuming that an ongoing location tracking warrant could be issued, without referencing the All Writs Act, and before enactment of the tracking device statute). And even if there were any prospective search authority under the All Writs Act, it would be displaced by the more specific time limits imposed by Rule 41. See *Penn. Bureau of Correction v. United States Marshals Serv.*, 474 U.S. 34, 40-43 (1985) (emphasizing that the All Writs Act is a “residual source of authority” that is overridden by more specific provisions).

<sup>132</sup> FED R. CRIM. P. 41(e)(2)(C) (setting out time limits for installation and operation of a location tracking device pursuant to a warrant). Before federal and state rules were

considered for government malware.

*D. When and how must the government provide notice of hacking?*

Since the framing era, courts have imposed both *ex ante* and *ex post* notice requirements on law enforcement searches.<sup>133</sup> Pre-execution notice, often dubbed “knock-and-announce,” minimizes the disruption and damage associated with conducting a search.<sup>134</sup> The Supreme Court’s most recent notice guidance, in *Wilson v. Arkansas*, explained that *ex ante* notice is “an element of the reasonableness inquiry under the Fourth Amendment.”<sup>135</sup>

*Ex post* notice serves different policy aims; it facilitates transparency and promotes confidence in government investigative practices, ensuring that law enforcement officers comply with legal constraints.<sup>136</sup> Some courts have located an after-the-fact notice requirement in the Fourth Amendment itself,<sup>137</sup> while others have traced it to the Federal Rules of Criminal Procedure.<sup>138</sup>

Applying *ex ante* notice doctrine to government hacking is easy. Where law enforcement is conducting an ongoing investigation, the courts and Congress have consistently permitted electronic surveillance without pre-execution announcement. A rule to the contrary would frustrate the very purpose of the investigation, tipping off suspects and preventing collection of evidence.<sup>139</sup> Wiretap super-warrants and location tracking warrants are

---

amended to address tracking devices, the ordinary law enforcement practice was to obtain a series of time-limited warrants (if they obtained warrants at all). *See, e.g.*, *State v. Jackson*, 76 P.3d 217, 220-21 (Wash. 2003) (describing a ten-day tracking device warrant, followed by a second ten-day warrant).

<sup>133</sup> *See* Jonathan Witmer-Rich, *The Rapid Rise of Delayed Notice Searches*, 41 PEP. L. REV. 509, 561-70 (2014) (reviewing an unbroken history of search notice requirements); *see also* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 803 (1994) (describing *ex post* notice as a central feature of Fourth Amendment warrants).

<sup>134</sup> *See* *Wilson v. Arkansas*, 514 U.S. 927, 931-34 (1995) (explaining historical policy rationales for *ex ante* search notice).

<sup>135</sup> *Id.* at 934.

<sup>136</sup> *See generally* Brian L. Owsley, *To Unseal or Not to Unseal: The Judiciary’s Role in Preventing Transparency in Electronic Surveillance Applications and Orders*, 5 CAL. L. REV. CIR. 259 (2014) (discussing policy concerns associated with sealed surveillance orders).

<sup>137</sup> *See, e.g.*, *Untied States v. Freitas*, 800 F.2d 1451, 1456 (9th Cir. 1986) (holding that the Fourth Amendment mandates *ex post* notice with minimum delay); *see also* *Berger v. New York*, 388 U.S. 41, 60 (1967) (describing notice as a “requirement” for “conventional warrants.”).

<sup>138</sup> *See, e.g.*, *United States v. Pangburn*, 983 F.2d 449, 449-50 (2d Cir. 1993) (“Although we have required that seven days notice be given after covert entries for which search without physical seizure has been authorized, that notice requirement is grounded in Fed. R. Crim P. 41 and is not compelled by the Constitution.”).

<sup>139</sup> *See* *Berger v. New York*, 388 U.S. 41, 86 (1967) (Black, J., dissenting) (noting the



regularly issued with delayed notice, and Congress has provided general authority for delayed notice (“sneak and peek”) warrants.<sup>140</sup> The same procedure should be constitutionally permissible for government malware.

Ex post notice is the much greater challenge. Is it required? Who receives the notice? How must it be provided? I establish the principles for each of these subsidiary issues, then match the resulting standard against current government practice.

Whether mandated by the Fourth Amendment or not, Rule 41 and its associated statutes are textually unambiguous. The government must *eventually* provide notice of a search warrant’s execution.<sup>141</sup> Courts do have broad, case-specific discretion to delay notice—but there must, ultimately, be notice. Hacking warrants, then, are subject to an ex post notice requirement.

The recipient of warrant notice is usually the person with a privacy interest in the target of the search or seizure. Courts have relaxed that requirement, under both the Fourth Amendment and Rule 41, where property or data is in the possession of a third-party business. Searches of parcels in transit, for instance, have been held permissible with notice solely to the shipping company.<sup>142</sup> Searches of electronic content, stored with a cloud service provider, are similarly allowed with notice only to the third-party business.<sup>143</sup> When executing a hacking warrant, though, these third-party

---

futility of ex ante notice for electronic surveillance).

<sup>140</sup> 18 U.S.C. § 2518(8)(d) (requiring actual service of notice within 90 days of a wiretap’s conclusion); 18 U.S.C. § 3103a (general authority for delayed notice search and seizure warrants); FED. R. CRIM. P. 41(f)(3) (permitting issuance of delayed notice warrants, where authorized by statute).

<sup>141</sup> See Letter from Assistant Attorney General William E. Moschella to Speaker of the House of Representatives J. Dennis Hastert, at 7 (July 25, 2003), *available at* <https://cdt.org/files/security/usapatriot/030725doj.pdf> (explaining that the delayed-notice search statute “requires law enforcement to give notice that a search warrant has been executed in *all circumstances*”); *cf.* In Re Grand Jury Subpoena for [Redacted]@yahoo.com, No. 5:15-cr-90096-PSG, 2015 U.S. Dist. LEXIS 17379 (N.D. Cal. Feb. 5, 2015) (rejecting indefinite gag orders for electronic data warrants and subpoenas).

<sup>142</sup> See, e.g., *United States v. Zacher*, 465 F.3d 336, 339 (9th Cir. 2006) (permitting notice of a package seizure by leaving a receipt with FedEx).

<sup>143</sup> The Stored Communications Act (SCA) does not statutorily require notice to a subscriber after the government executes a search warrant for content stored with a service provider. 18 U.S.C. § 2703. Courts disagree on whether SCA expressly eliminates any notice requirement, or merely defers to the notice provisions of Rule 41. *Compare* *United States v. Scully*, No. 14-CR-208 (ADS)(SIL), 2015 U.S. Dist. LEXIS 73831, at \*48-59 (E.D.N.Y. June 8, 2015) (concluding that the SCA only mandates notice where investigators have not obtained a warrant) *with* *In Re Application of the United States for an Order*, 665 F. Supp. 2d 1210, 1216-21 (D. Or. 2009) (holding that the SCA incorporates Rule 41, including its notice provisions). Furthermore, at the time the SCA was enacted, Congress (and the courts) believed that content stored with a third-party business was exempt from Fourth Amendment protection. See *United States v. Warshak*, 631 F. 3d 266 (6th Cir. 2010) (concluding that the SCA violates the Fourth Amendment by not imposing a warrant requirement for content

notice cases are not applicable; the government is conducting a search of the suspect's *own* computer system, by directly breaking into it. The notice associated with a hacking warrant, then, must be directed to the suspect him- or herself.

In a conventional search, actual notice is provided by furnishing a copy of the warrant (and a receipt for anything taken).<sup>144</sup> Wiretap super-warrants and location tracking warrants are usually also followed by actual notice.<sup>145</sup> The Fourth Amendment and Rule 41 do permit for constructive notice, though; investigators may leave a copy of a warrant at the site of the search or seizure.<sup>146</sup> This same minimum would apply to a hacking warrant; it must, at least, be accompanied by constructive notice.

When the government executes a hacking warrant for a known computer, it appears to comport with these three requirements.<sup>147</sup> It provides eventual notice, to the computer's owner, through actual (not just constructive) service.

When the government deploys identification malware, by contrast, it presently falls far short of the three requirements. The current practice is to not *ever* provide notice of hacking, to *any* affected person, in *any* form, until subsequent investigation discloses the identity of a hacked computer's likely owner. In more precise legal terms, the government believes it can

---

privately stored with third-party services). In a modern understanding, then: a warrant for content stored with a service provider must satisfy the notice requirements of the Fourth Amendment (to the extent they exist) and Rule 41 (to the extent they are not uniquely abrogated by the SCA). These notice requirements are both satisfied because the warrant is executed via a third party. *See* In Re Application of the United States for an Order, 665 F. Supp. 2d 1210, 1221-22 (D. Or. 2009) (holding that a warrant for stored content, executed via a third-party service provider, satisfies Rule 41's notice requirements); *id.* at 1222-24 (same for Fourth Amendment's notice requirement).

<sup>144</sup> FED R. CRIM. P. 41(f)(1)(C) ("The officer executing the warrant must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken . . .").

<sup>145</sup> 18 U.S.C. § 2518 ("[T]he issuing or denying judge shall cause to be served, on the persons named in the order or the application, and such other parties to intercepted communications as the judge may determine in his discretion that is in the interest of justice, an inventory [of the wiretap application and execution]."); FED R. CRIM. P. 41(f)(2)(C) ("[T]he officer executing a tracking-device warrant must serve a copy of the warrant on the person who was tracked or whose property was tracked. Service may be accomplished by delivering a copy to the person who, or whose property, was tracked . . .").

<sup>146</sup> FED R. CRIM. P. 41(f)(1)(C) (allowing constructive notice of a search or seizure warrant by "leav[ing] a copy of the warrant and receipt at the place where the officer took the property"); *see also* FED R. CRIM. P. 41(f)(2)(C) (allowing constructive notice of a tracking device warrant "by leaving a copy at the person's residence or usual place of abode with an individual of suitable age and discretion who resides at that location and by mailing a copy to the person's last known address").

<sup>147</sup> *See, e.g.,* United States v. Scarfo, 180 F. Supp. 2d 572, 574-575 (D.N.J. 2001) (providing timeline for FBI investigation).

particularly describe a computer to hack, but cannot reasonably describe a place to leave notice or a person to send notice.

Recent hacking warrant applications uniformly rely upon this type of conditional *ex post* notice.<sup>148</sup> The operational consequence is that the government can hack with no transparency, until it elects to subpoena a particular hacked user's Internet service provider for subscriber information. That result poses extraordinary privacy risk: the government can hack a large number of computers and then, in its *exclusive* discretion, furnish *ex post* notice to their owners.

This is, unfortunately, not a hypothetical. In a 2013 investigation, discussed above, the FBI deployed identification malware on seized webservers.<sup>149</sup> The FBI's watering hole strategy extended far beyond child pornography websites, reaching a number of non-criminal services—including a popular email provider.<sup>150</sup> Because of its position on hacking warrant notice, though, the FBI was able to escape legal repercussions. Thousands of innocent American users (if not more) likely had their Fourth Amendment rights violated, and may have had meritorious claims for damages. But they never learned that their computer was breached, because the FBI never subpoenaed for their identities.

The ideal resolution for hacking warrant notice would be a clarifying amendment to Rule 41. The rule already includes special notice procedures

---

<sup>148</sup> Second Amended Application and Third Amended Affidavit of FBI Task Force Officer William A. Gallegos for a Network Investigative Technique Warrant, No. 12-sw-05685-KMT, at 24 (D. Colo. Dec. 11, 2013) (specifying that “the government may delay providing a copy of the search warrant and the receipt for any property taken until the time that a suspect has been identified and has been placed in custody”); Application and Affidavit of FBI Special Agent Justin E. Noble for a Network Investigative Technique Warrant, No. 1:12-mj-00748-ML, at 13 (W.D. Tex. Dec. 18, 2012) (requesting delayed notice “because the investigation has not identified an appropriate person to whom such notice can be given”); Application and Affidavit of FBI Special Agent Jeffrey Tarpinian for a Network Investigative Technique Warrant, No. 8:12MJ356, at 35-36 (D. Neb. Nov. 16, 2012) (specifying that “the government may delay providing a copy of the search warrant and the receipt for any property taken for thirty (30) days after a user of an ‘activating’ computer that accessed ‘Bulleting Board A’ has been identified to a sufficient degree as to provide notice”); Application and Affidavit of FBI Special Agent Norman B. Sanders for a Computer and Internet Protocol Address Verifier Warrant, No. MJ07-5114, at 16 (W.D. Wash. June 12, 2007) (specifying that “the FBI may delay providing a copy of the search warrant and the receipt for any property taken until no more than thirty (30) days after such time as the name and location of the individual(s) using the activating computer is positively identified”).

<sup>149</sup> See Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, WIRED (Sept. 13, 2013), <http://www.wired.com/2013/09/freedom-hosting-fbi/>.

<sup>150</sup> See Kevin Poulsen, *If You Used This Secure Webmail Site, the FBI Has Your Inbox*, WIRED (Jan. 27, 2014), <http://www.wired.com/2014/01/tormail/>; Kevin Poulsen, *Feds Are Suspects in New Malware That Attacks Tor Anonymity*, WIRED (Aug. 5, 2013), <http://www.wired.com/2013/08/freedom-hosting/>.

for tracking devices; a similar set of provisions for government malware would lend much-needed clarity.<sup>151</sup>

Until then, though, judges should immediately cease issuing conditional notice hacking warrants. One stop-gap fix would be devising a constructive notice strategy, as is already contemplated by Rule 41. The government might change a hacked computer's desktop background, for instance, or provide a pop-up alert. Another direction would be ensuring actual notice, by requiring the government to subpoena a hacked computer's Internet service provider. Investigators could then guarantee actual notice through ordinary, in-person service.

I do not claim to have a fully satisfactory answer for how to design ex post notice for government malware. Both of these stop-gap suggestions have drawbacks.<sup>152</sup> But plainly the status quo is unsustainable, as a matter of policy, as a matter of Rule 41, and (possibly) as a matter of the Fourth Amendment.

*E. When does government malware require a super-warrant?*

In *Berger v. New York*, the Supreme Court indicated that the Fourth Amendment mandates "super-warrant" procedures for real-time communications interception.<sup>153</sup> As implemented in the Wiretap Act, the four core safeguards are: a determination that ordinary investigative techniques have failed or would likely be ineffective, a particular description of the communications sought, a firm time limit on the surveillance, and minimized interception of non-pertinent communications.<sup>154</sup> Additional requirements include an ongoing investigation into an enumerated serious offense, as well as prompt notice to the target.<sup>155</sup> The Wiretap Act also provides for an annual report on federal and state investigative practices.<sup>156</sup>

The *Berger* doctrine, and the Wiretap Act, plainly apply to phone wiretaps and audio bugs. If government malware activates a computer's microphone, or otherwise intercepts a private spoken conversation, then it unambiguously must be operated with a super-warrant.<sup>157</sup>

---

<sup>151</sup> See FED R. CRIM. P. 41(f)(2)(C) (special ex post notice provisions for tracking device warrants).

<sup>152</sup> The government might not want to leave malware resident on a suspect's computer longer than is necessary, for instance. And subpoenaing a person's identity is an extra (albeit slight) privacy intrusion.

<sup>153</sup> 388 U.S. 41, 58-60 (1967).

<sup>154</sup> 18 U.S.C. § 2518.

<sup>155</sup> *Id.*

<sup>156</sup> 18 U.S.C. § 2519.

<sup>157</sup> Letter from Deputy Assistant Attorney General David Bitkower to the Advisory Committee on the Federal Rules of Criminal Procedure, at 9 (Dec. 22, 2014) (noting that the

In the decades following *Berger*, a number of cases posed the question of how the Fourth Amendment regulates video surveillance.<sup>158</sup> The unanimous conclusion among federal appellate courts has been that the Wiretap Act does not apply, but the *Berger* doctrine does. Courts must, consequently, borrow the core super-warrant protections from the Wiretap Act when authorizing video surveillance. The result for law enforcement malware is clear guidance: if agents seek to enable a computer's camera, they must obtain a super-warrant in advance.<sup>159</sup> In at least one investigation, though, the FBI has failed to adhere to this requirement.<sup>160</sup>

Internet connectivity is a third easy-to-spot area of super-warrant coverage. Courts have consistently applied *Berger* and the Wiretap Act to real-time interception of online content.<sup>161</sup> If government malware intercepts content flowing through a computer's Wi-Fi, Bluetooth, Ethernet, or any other network interface, it must be installed and operated with a super-warrant.

A fourth fact pattern with unambiguous *Berger* and Wiretap Act coverage is where the government remotely monitors keystrokes or screen content, while the user is typing or receiving a communication.<sup>162</sup> That

---

real-time communications content interception provisions of the Wiretap Act remain applicability to government hacking).

<sup>158</sup> See *United States v. Williams*, 124 F.3d 411, 416-20 (3d Cir. 1997) (Alito, J.) (assuming the correctness of *Torres*); *United States v. Falls*, 34 F.3d 674, 678-83 (following and applying *Koyomejian*) (8th Cir. 1994); *United States v. Koyomejian*, 970 F.2d 536, 538-42 (9th Cir. 1992) (following *Cuevas-Sanchez*); *United States v. Mesa-Rincon*, 911 F.2d 1433, 1436-46 (10th Cir. 1990) (applying the four core protections of the Wiretap Act to video surveillance); *United States v. Cuevas-Sanchez*, 821 F.2d 248, 251-52 (5th Cir. 1987) (adopting *Biasucci* and *Torres*); *United States v. Biasucci*, 786 F.2d 504, 507-12 (2d Cir. 1986) (following *Torres*); *United States v. Torres*, 751 F.2d 875, 882-85 (7th Cir. 1984) (holding that the four core protections of the Wiretap Act are mandated by the Fourth Amendment for video surveillance, and the Federal Rules of Criminal Procedure are sufficiently flexible to accommodate those super-warrant safeguards).

<sup>159</sup> See *In Re Warrant to Search a Target Computer at Premises Unknown*, 958 F. Supp. 2d 753, 759-61 (S.D. Tex. 2013) (holding that the core *Berger* requirements apply to FBI malware that activates a computer's webcam).

<sup>160</sup> *Id.* (denying malware warrant, in part, for failing to adhere to the *Berger* requirements for video surveillance).

<sup>161</sup> See, e.g., *Joffe v. Google*, 746 F.3d 920, 926-36 (9th Cir. 2013) (wireless network interception); *United States v. Councilman*, 418 F.3d 67, 69-85 (9th Cir. 2005) (email interception). If the government obtains solely real-time communications metadata in conjunction with a hack, it must comport with the pen register statute. 18 U.S.C. §§ 3121-3127. Since a warrant is substantively more rigorous than a pen/trap order, the only practical implication is that a federal investigation must be included in an annual Department of Justice pen/trap report. 18 U.S.C. § 3126.

<sup>162</sup> See *Luis v. Zang*, No. 1:11-cv-884, 2013 WL 811816, at \*12-25 (S.D. Ohio, Mar. 5, 2013) (reviewing litigation on keyloggers and concluding that, if malware reports keystrokes to a remote party, it implicates the Wiretap Act); *Shefts v. Petrakis*, No. 10-cv-1104, 2012

communication could be among individuals, such as an email or instant message, or it could be with a business, such as loading a webpage. When computer systems were only temporarily connected to the Internet, via modem, the government was (arguably) able to evade heightened wiretapping requirements.<sup>163</sup> Given the modern reality of always-on Internet connectivity, though, keystroke logging and screen capturing malware will generally require a super-warrant.

Outside of these four areas, the applicability of super-warrant doctrine to government hacking remains entirely unsettled. How should the courts, and Congress, more generally reconcile *Berger* and the Wiretap Act with government malware? The following Conclusion takes a step back, and offers normative arguments in favor of malware super-warrants.

#### CONCLUSION: IN FAVOR OF MALWARE SUPER-WARRANTS

The government's track record with law enforcement hacking is hardly stellar. Descriptions of hacking practices are deliberately ambiguous (Introduction). Investigators sometimes assert that no warrant is required at all (Parts I, II.A). Probable cause and particularity have previously been botched, with malware delivered to innocent users (Part II.B). Warrant applications ignore the unambiguous time limits of Rule 41 (Part II.C). Every public warrant for identification malware relies upon conditional notice, in violation of Rule 41 and (possibly) the Fourth Amendment (Part II.D). And, finally, the government has not properly applied for a super-warrant in scenarios where they are unambiguously required (Part II.E). This string of procedural defects should weigh heavily in favor of heightened judicial scrutiny.

Similar considerations prompted the development of wiretapping doctrine in the 1960s. Writing for the majority in *Berger*, Justice Clark acknowledged that telephone wiretaps and audio bugs could be potent investigative techniques.<sup>164</sup> But he also emphasized that legislation and

---

U.S. Dist. LEXIS 130542, at \*37-43 (C.D. Ill., Sept. 12, 2012) (holding that screen capture software that recorded email activity was covered by the Wiretap Act). Courts have generally not required that the transmission of recorded activity be precisely contemporaneous with the activity. *See Williams v. Stoddard*, No. PC 12-3664, 2015 R.I. Super. LEXIS 58, at \*19-30 (R.I. Super. Ct. Feb. 11, 2015) (summarizing perspectives on wiretap timing).

<sup>163</sup> *See United States v. Scarfo*, 180 F. Supp. 2d 572, 581-82 (D.N.J. 2001) (declining to apply the Wiretap Act to government malware which was configured to only operate when the computer's modem).

<sup>164</sup> 388 U.S. 41, 46 (1967) ("During prohibition days wiretaps were the principal source of information relied upon by the police as the basis for prosecutions."). The majority did express skepticism, though, about whether eavesdropping evidence was necessary for law enforcement. *Id.* at 60-63.

jurisprudence had failed to keep up with technological advances, and investigators had exceeded the scope of even clearly established safeguards.<sup>165</sup> Both of those policy factors favor extending super-warrant doctrine to government hacking.

A concurring opinion by Justices Douglas and Stewart highlights an additional policy motivation for super-warrant doctrine. Electronic surveillance raises the specter of the “invisible policeman,” they wrote.<sup>166</sup> “[I]t is the greatest of all invasions of privacy. It places a government agent in the bedroom, in the business conference, in the social hour, in the lawyer’s office—everywhere and anywhere a ‘bug’ can be placed.”<sup>167</sup>

These justices surely could not have imagined modern information technology. Americans already carry around “minicomputers” in their pockets and on their wrists, replete with audio, video, and location sensors.<sup>168</sup> Government agents need not “place” any monitoring gear of their own; rather, they can subvert already-ubiquitous sensors and storage devices. If the potential for omnipresent state surveillance is a criterion for super-warrant doctrine, it is difficult to imagine a more qualifying investigative technique than government hacking.

The risk of dragnet data collection is another rationale for imposing super-warrant requirements on law enforcement malware. Courts have emphasized that surreptitious audio and video surveillance tend to record innocent individuals and non-criminal conduct.<sup>169</sup> Law enforcement hacking

---

<sup>165</sup> *Id.* (“Some 50 years ago a New York legislative committee found that police, in cooperation with the telephone company, had been tapping telephone lines in New York despite an Act passed in 1895 prohibiting it.”); *id.* at 49 (“The law, though jealous of individual privacy, has not kept pace with these advances in scientific knowledge.”).

<sup>166</sup> *Id.* at 65 (Douglas, J., concurring).

<sup>167</sup> *Id.* at 64-65.

<sup>168</sup> *See Riley v. California*, 134 S. Ct. 2473, 2489 (2014) (“The term ‘cell phone’ is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.”).

<sup>169</sup> *See Berger*, 488 U.S. at 49 (majority opinion) (“[T]he conversations of any and all persons coming into the area covered by the device will be seized indiscriminately and without regard to their connection with the crime under investigation.”); *id.* at 65 (Douglas, J., concurring) (“The traditional wiretap or electronic eavesdropping device constitutes a dragnet, sweeping in all conversations within its scope—without regard to the participants or the nature of the conversations. It intrudes upon the privacy of those not even suspected of crime and intercepts the most intimate of conversations.”); *United States v. Biasucci*, 762 F.2d 504, 510 (2d Cir. 1986) (“[C]oncern with the indiscriminate nature of electronic surveillance led the *Berger* Court to require that a warrant authorizing electronic surveillance be sufficiently precise so as to minimize the recording of activities not related to the crimes under investigation.”); *United States v. Torres*, 751 F.2d 875, 885 (7th Cir. 1984) (“Television surveillance is identical *in its indiscriminate character* to wiretapping and

poses dragnet risks, too, albeit in somewhat different manner. Unlike with audio and video surveillance, the government can explicitly constrain the types of information that it receives. But, much like with audio and video recording, the government's investigative technique might affect the privacy interests of innocent (virtual) bystanders. And, because software scales so easily, the magnitude of collateral surveillance can be—and has been—extraordinary. Under a super-warrant regime, investigators would have to much more explicitly scope the devices they will hack and the information they will obtain.

A super-warrant mandate would also serve a beneficial channeling function. In many modern investigations, the government can obtain data through multiple means—by serving a warrant on a cloud service, by physically seizing a suspect's computer, by breaking into the suspect's cloud account, or by hacking the suspect's computer. Warrants served on technology companies are preferable; they allow for regular transparency reporting, and they impose an added independent, impartial intermediary between the government and a wealth of user data.<sup>170</sup> Computer seizures are the next best option; they result in forensic analysis of a disk image, accompanied by a detailed log of investigative queries. Hacking techniques could circumvent these valuable transparency and review procedures, replacing them with ad hoc investigative practice. The necessity component of *Berger's* super-warrant test would require the government to justify why a cloud service warrant or a physical device seizure wouldn't work, before sanctioning a hack.

Predictability is another virtue of the super-warrant approach. The alternative would be carefully parsing the information that law enforcement obtains via hacking warrants, nitpicking which categories of data fall on which side of the super-warrant line. However difficult that approach may be today, it will only be more complex in future. As more and more device functionality incorporates an online component—from applications to

---

bugging.”).

<sup>170</sup> See NATE CARDOZO ET AL., ELEC. FRONTIER FOUND., WHO HAS YOUR BACK? (2015), available at [https://www.eff.org/files/2015/06/18/who\\_has\\_your\\_back\\_2015\\_protecting\\_your\\_data\\_from\\_government\\_requests\\_20150618.pdf](https://www.eff.org/files/2015/06/18/who_has_your_back_2015_protecting_your_data_from_government_requests_20150618.pdf) (collecting business policies for handling government data demands, including annual transparency reports); Google, *Way of a Warrant*, YOUTUBE (Feb. 10, 2009), <https://www.youtube.com/watch?v=MeKKHxcJfh0> (explaining that Google requires search warrants for user content, examines warrants for errors, narrows production for overbroad warrants, and notifies users of government demands); see, e.g., Opening Brief of Appellant Facebook, Inc., In Re 381 Search Warrants Directed to Facebook, Inc. and Dated July 23, 2013, No. 30207-13 (N.Y. Sup. Ct. App. Div. June 20, 2014) (Facebook challenge to New York County District Attorney search warrants for user content with questionable probable cause support and no date or content restrictions).



operating systems—courts would be left to arbitrarily delineate between warrant and super-warrant hacking.<sup>171</sup>

Externalities are yet another reason for adopting super-warrants. In the wake of recent foreign intelligence disclosures, trust in information technology has become a critical commercial concern; recent estimates place costs to American businesses at tens of billions of dollars.<sup>172</sup> With each episode of government hacking, investigators impose real economic consequences that they do not internalize. A super-warrant requirement forces a degree of internalization, requiring extra detail and justification in the surveillance application.

Even if courts decline to find this normative argumentation persuasive, Congress still could. It would be trivial to statutorily impose super-warrant requirements on law enforcement hacking. Legislation could simply combine the hacking definition from the Computer Fraud and Abuse Act with the super-warrant procedure from the Wiretap Act.

In closing, I wish to reiterate: I believe that hacking can be a legitimate and effective law enforcement technique. I take no issue with the government possessing tools for compromising computer systems. But appropriate procedural protections are vital, and present practices leave much room for improvement.

---

<sup>171</sup> A hypothetical: imagine that the government hacks a user's device and monitors their files. So far, courts have concluded that super-warrant doctrine does not apply. But moving forward a user's files will be automatically synced to remote services and other devices (e.g. Apple's iCloud). Those are plainly electronic communications under the Wiretap Act and the *Berger* doctrine. Would the government then be required to obtain a super-warrant for file monitoring?

<sup>172</sup> See ED FERRERA ET AL., FORRESTER RESEARCH, GOVERNMENT SPYING WILL COST US VENDORS FEWER BILLIONS THAN INITIAL ESTIMATES (2015) (estimating \$47 billion in costs); Daniel Castro & Alan McQuinn, Info. Tech. & Innovation Found., Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness (June 2015), <http://www2.itif.org/2015-beyond-usa-freedom-act.pdf> (estimating \$35 billion in costs).

2014

## Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet

Steven M. Bellovin  
*Columbia University*

Matt Blaze  
*University of Pennsylvania*

Sandy Clark  
*University of Pennsylvania*

Susan Landau  
*privacyink.org, susan.landau@privacyink.org*

---

### Recommended Citation

Steven M. Bellovin, Matt Blaze, Sandy Clark, and Susan Landau, *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 *Nw. J. Tech. & Intell. Prop.* 1 (2014).  
<http://scholarlycommons.law.northwestern.edu/njtp/vol12/ss1/1>

This Article is brought to you for free and open access by Northwestern University School of Law Scholarly Commons. It has been accepted for inclusion in Northwestern Journal of Technology and Intellectual Property by the authorized administrator of Northwestern University School of Law Scholarly Commons.

N O R T H W E S T E R N  
JOURNAL OF TECHNOLOGY  
AND  
INTELLECTUAL PROPERTY

**Lawful Hacking:  
Using Existing Vulnerabilities for  
Wiretapping on the Internet**

*Steven M. Bellovin, Matt Blaze, Sandy Clark, & Susan Landau*



---

April 2014

VOL. 12, NO. 1

# Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet

By Steven M. Bellovin<sup>\*</sup>, Matt Blaze<sup>†</sup>, Sandy Clark<sup>§</sup>, & Susan Landau<sup>‡</sup>

*For years, legal wiretapping was straightforward: the officer doing the intercept connected a tape recorder or the like to a single pair of wires. By the 1990s, however, the changing structure of telecommunications—there was no longer just “Ma Bell” to talk to—and new technologies such as ISDN and cellular telephony made executing a wiretap more complicated for law enforcement. Simple technologies would no longer suffice. In response, Congress passed the Communications Assistance for Law Enforcement Act (CALEA)<sup>1</sup>, which mandated a standardized lawful intercept interface on all local phone switches. Since its passage, technology has continued to progress, and in the face of new forms of communication—Skype, voice chat during multiplayer online games, instant messaging, etc.—law enforcement is again experiencing problems. The FBI has called this “Going Dark”: their loss of access to suspects’ communication.<sup>2</sup> According to news reports, law enforcement wants changes to the wiretap laws to require a CALEA-like interface in Internet software.<sup>3</sup>*

*CALEA, though, has its own issues: it is complex software specifically intended to create a security hole—eavesdropping capability—in the already-complex environment of a phone switch. It has unfortunately made wiretapping easier for everyone, not just law enforcement. Congress failed to heed experts’ warnings of the danger posed by this mandated vulnerability, and time has proven the experts right. The so-called “Athens Affair,” where someone used the built-in lawful intercept mechanism to listen to the cell phone calls of high Greek officials, including the Prime Minister,<sup>4</sup> is but one example. In an earlier work, we showed why extending CALEA to the Internet would create very serious problems, including the security problems it has visited on the phone system.<sup>5</sup>*

---

<sup>\*</sup> Steven M. Bellovin is a professor of computer science at Columbia University.

<sup>†</sup> Matt Blaze is an associate professor of computer science at the University of Pennsylvania.

<sup>§</sup> Sandy Clark is a Ph.D. student in computer science at the University of Pennsylvania.

<sup>‡</sup> Susan Landau was a 2012 Guggenheim Fellow; she is now at [privacyink.org](http://privacyink.org).

<sup>1</sup> Pub. L. No. 103-414, 108 Stat. 4279 (codified at 47 U.S.C. §§ 1001–1010 (2006)).

<sup>2</sup> *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. On Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 10 (2011) (prepared statement of Valerie Caproni, General Counsel, Federal Bureau of Investigation), available at [http://judiciary.house.gov/hearings/printers/112th/112-59\\_64581.PDF](http://judiciary.house.gov/hearings/printers/112th/112-59_64581.PDF).

<sup>3</sup> Declan McCullagh, ‘Dark’ Motive: FBI Seeks Signs of Carrier Roadblocks to Surveillance, CNET (Nov. 5, 2012, 1:03 PM), [http://news.cnet.com/8301-13578\\_3-57545353-38/dark-motive-fbi-seeks-signs-of-carrier-roadblocks-to-surveillance/](http://news.cnet.com/8301-13578_3-57545353-38/dark-motive-fbi-seeks-signs-of-carrier-roadblocks-to-surveillance/).

<sup>4</sup> Vassilis Prevelakis & Diomidis Spinellis, *The Athens Affair*, IEEE SPECTRUM, July 2007, at 27, available at <http://spectrum.ieee.org/telecom/security/the-athens-affair/0>.

<sup>5</sup> Steven M. Bellovin, Matt Blaze, Sandy Clark & Susan Landau, *Going Bright: Wiretapping Without Weakening Communications Infrastructure*, IEEE SECURITY & PRIVACY, Jan/Feb 2013, at 64–66, available at <https://www.cs.columbia.edu/~smb/papers/GoingBright.pdf>.

*In this paper, we explore the viability and implications of an alternative method for addressing law enforcements need to access communications: legalized hacking of target devices through existing vulnerabilities in end-user software and platforms. The FBI already uses this approach on a small scale; we expect that its use will increase, especially as centralized wiretapping capabilities become less viable.*

*Relying on vulnerabilities and hacking poses a large set of legal and policy questions, some practical and some normative. Among these are:*

- (1) Will it create disincentives to patching?*
- (2) Will there be a negative effect on innovation? (Lessons from the so-called “Crypto Wars” of the 1990s, and in particular the debate over export controls on cryptography, are instructive here.)*
- (3) Will law enforcement’s participation in vulnerabilities purchasing skew the market?*
- (4) Do local and even state law enforcement agencies have the technical sophistication to develop and use exploits? If not, how should this be handled? A larger FBI role?*
- (5) Should law enforcement even be participating in a market where many of the sellers and other buyers are themselves criminals?*
- (6) What happens if these tools are captured and repurposed by miscreants?*
- (7) Should we sanction otherwise illegal network activity to aid law enforcement?*
- (8) Is the probability of success from such an approach too low for it to be useful?*

*As we will show, these issues are indeed challenging. We regard the issues raised by using vulnerabilities as, on balance, preferable to adding more complexity and insecurity to online systems.*

I.	INTRODUCTION .....	3
II.	CALEA: THE CHANGE IN WIRETAP ARCHITECTURE .....	6
A.	History of CALEA .....	7
B.	Wiretap Consequences of Splitting Services and Infrastructure.....	9
C.	New Technologies: Going Dark or Going Bright? .....	13
D.	The TPWG's Tracking Preferences Expression Standard .....	17
III.	THE VULNERABILITY OPTION .....	22
A.	Definition of Terms.....	23
B.	How Vulnerabilities Help .....	24
C.	Why Vulnerabilities Will Always Exist .....	27
D.	Why the Vulnerability Solution Must Exist Anyway .....	30
IV.	VULNERABILITY MECHANICS.....	31
A.	Warrant Issues.....	31
B.	Architecture.....	32
C.	Technical Aspects of Minimization .....	33
D.	Technical Reconnaissance .....	36
E.	Finding Vulnerabilities .....	37
F.	Exploits and Productizing.....	39
G.	The Vulnerabilities Market.....	41
V.	PREVENTING PROLIFERATION.....	44
A.	Public Policy Concerns in Deploying Exploits to Wiretap.....	44
B.	Ethical Concerns of Exploiting Vulnerabilities to Wiretap .....	47
C.	Technical Solutions to Preventing Proliferation .....	49
VI.	REPORTING VULNERABILITIES.....	50
A.	Security Risks Created by Using Vulnerabilities.....	50
B.	Preventing Crime .....	51
C.	A Default Obligation to Report.....	56
VII.	EXECUTIVE AND LEGISLATIVE ENFORCEMENT .....	58
A.	Enforcing Reporting.....	58
B.	Exceptions to the Reporting Rule .....	59
C.	Providing Oversight.....	61
D.	Regulating Vulnerabilities and Exploitation Tools.....	62
VIII.	CONCLUSION.....	64

## I. INTRODUCTION

¶1 For several years, the FBI has warned that newer communications technologies have hindered its ability to conduct electronic surveillance.<sup>6</sup> Valerie Caproni, General Counsel of the FBI, said in Congressional testimony:

---

<sup>6</sup> See, e.g., *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*, *supra* note 2

Methods of accessing communications networks have similarly grown in variety and complexity. Recent innovations in hand-held devices have changed the ways in which consumers access networks and network-based services. One result of this change is a transformation of communications services from a straightforward relationship between a customer and a single CALEA-covered provider (e.g. customer to telephone company) to a complex environment in which a customer may use several access methods to maintain simultaneous interactions with multiple providers, some of whom may be based overseas or are otherwise outside the scope of CALEA.

As a result, although the government may obtain a court order authorizing the collection of certain communications, it often serves that order on a provider who does not have an obligation under CALEA to be prepared to execute it.<sup>7</sup>

¶2 The FBI's solution is "legislation that will assure that when we get the appropriate court order . . . companies . . . served . . . have the capability and the capacity to respond."<sup>8</sup>

¶3 While on the one hand this request is predictable given past precedent, it is rather remarkable given current national cybersecurity concerns and in light of stark evidence of the significant harm caused by CALEA. The request to expand CALEA to IP-based communications places the needs of the Electronic Surveillance Unit above all else, including the security risks that arise when building wiretapping capabilities into communications infrastructure and applications, other government agencies who face increased risk from hackers and nation states who may exploit this new vulnerability, and the national need for innovation which drives economic prosperity. Rather than examine the issue in terms of social good—which the FBI already does each time it prioritizes certain types of investigations (terrorism cases, drug cases, etc.) or decides whether to conduct a particular investigation—the FBI has thrown down a gauntlet that ignores long-term national interest.

¶4 The FBI's preferred solution—"requiring that social-networking Web sites and providers of VoIP, instant messaging, and Web e-mail alter their code to ensure their products are wiretap-friendly"<sup>9</sup>—will create security risks in our already-fragile Internet infrastructure, leaving the nation more vulnerable to espionage and our critical infrastructure more open to attack, and hinder innovation.<sup>10</sup> Securing communications infrastructure is a national priority. By weakening communications infrastructure and

---

(prepared statement of Valerie Caproni, General Counsel, Federal Bureau of Investigation). The FBI is the law-enforcement agency with the greatest role for setting policy on wiretapping.

<sup>7</sup> *Id.* at 14.

<sup>8</sup> See Oversight of the Federal Bureau of Investigation: Hearing Before the S. Comm. on the Judiciary, 112th Congress (2012) (statement of Robert S. Mueller, III, Director, Federal Bureau of Investigation); see also Declan McCullagh, *FBI 'Looking at' Law Making Web Sites Wiretap-Ready, Director Says*, CNET (May 18, 2012, 1:17 PM), [http://news.cnet.com/8301-1009\\_3-57437391-83/fbi-looking-at-law-making-web-sites-wiretap-ready-director-says/](http://news.cnet.com/8301-1009_3-57437391-83/fbi-looking-at-law-making-web-sites-wiretap-ready-director-says/).

<sup>9</sup> Declan McCullagh, *FBI: We Need Wiretap-Ready Web Sites—Now*, CNET (May 4, 2012, 9:34 AM), [http://news.cnet.com/8301-1009\\_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now/](http://news.cnet.com/8301-1009_3-57428067-83/fbi-we-need-wiretap-ready-web-sites-now/).

<sup>10</sup> Sometimes, such a solution directly benefits the U.S. military. One NSA program—Commercial Solutions for Classified—uses products from government research "layered" with private-sector products to produce communication tools with high security. See Fred Roeper & Neal Ziring, Presentation at RSA Conference 2012, Building Robust Security Solutions Using Layering and Independence 2–6 (2012), available at [http://www.rsaconference.com/writable/presentations/file\\_upload/star-401.pdf](http://www.rsaconference.com/writable/presentations/file_upload/star-401.pdf). However, this protection does not extend to the vast majority of civilian computers.

applications, the FBI's proposal would mostly give aid to the enemy. Surely that is neither what the FBI intends nor what sound national priorities dictate.

¶5 The problem is created by technology. Over the course of the last three decades, we have moved from a circuit-switched centralized communications network—the Public Switched Telephone Network (PSTN)—run by a monopoly provider, to a circuit-switched centralized communications network run by multiple providers, to an Internet-Protocol (IP) based decentralized network run by thousands of providers. The first change, from the monopoly provider to multiple providers, gave rise to the need for the Communications Assistance for Law Enforcement Act (CALEA). This simplified law enforcement's efforts to manage wiretaps with multiple, though relatively few, providers. However, in certain situations, such as when peer-to-peer communications or communications encrypted end-to-end are used, legally authorized wiretaps may be impeded. Even if law enforcement does not currently have a serious problem in conducting authorized wiretaps, with time it will. Thus, there is a serious question of what is to be done. In proposing controls on peer-to-peer networks and on the use of encryption,<sup>11</sup> the FBI has floated highly flawed solutions.<sup>12</sup>

¶6 We propose an alternative to the FBI's proposal: Instead of building wiretapping capabilities into communications infrastructure and applications, government wiretappers can behave like the bad guys. That is, they can exploit the rich supply of security vulnerabilities already existing in virtually every operating system and application to obtain access to communications of the targets of wiretap orders.<sup>13</sup>

¶7 We are not advocating the creation of *new* security holes,<sup>14</sup> but rather observing that exploiting *those that already exist* represents a viable—and significantly better—alternative to the FBI's proposals for mandating infrastructure insecurity. Put simply, the choice is between formalizing (and thereby constraining) the ability of law enforcement to occasionally use existing security vulnerabilities—something the FBI and other law enforcement agencies already do when necessary without much public or legal scrutiny—or living with those vulnerabilities *and* intentionally and systematically creating a set of predictable new vulnerabilities that despite best efforts will be exploitable by *everyone*.

¶8 Using vulnerabilities to create exploits and wiretap targets, however, raises ethical issues. Once an exploit for a particular security vulnerability leaves the lab, it may be used for other purposes and cause great damage. Any proposal to use vulnerabilities to enable wiretaps must minimize such risks.

¶9 In a previous work, we discussed the technical feasibility of relying on the vulnerability approach;<sup>15</sup> here we focus on the legal and policy issues posed by this

---

<sup>11</sup> See Charlie Savage, *U.S. is Working to Ease Wiretaps on the Internet*, N.Y. TIMES, Sept. 27, 2010, at A1.

<sup>12</sup> *Id.* Six months after the New York Times reported the FBI was seeking additional capabilities for Internet wiretapping, FBI General Counsel Valerie Caproni testified, “Congressman, the Administration is still working on what the solution would be, and we hope to have something that we can work with Congress on in the near future.” See *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*, *supra* note 2, at 40. As of this writing, no bill has been proposed.

<sup>13</sup> See Bellovin, Blaze, Clark & Landau, *supra* note 5, at 62–63.

<sup>14</sup> That is far from the case. Some of the authors have devoted much of their professional careers to preventing or coping with security holes and the problems they cause.

<sup>15</sup> See Bellovin, Blaze, Clark, & Landau, *supra* note 5, at 66–68.



approach. In particular, we examine the tension between the use of naturally occurring software vulnerabilities to legitimately aid law enforcement investigations and the abuse of the same vulnerabilities by criminals. We propose that law enforcement adopt strict guidelines requiring immediate disclosure to the vendor any vulnerabilities as soon they are discovered. As we will discuss, such guidelines would allow law enforcement to fully support crime prevention, and—because of the natural lag of the software lifecycle—still allow law enforcement to build a sufficiently rich toolkit to conduct investigations in practice.

¶10 The discussion in this paper is limited to use of vulnerabilities for *communications intercepts*, rather than generic “remote search.” While the two concepts have much in common, including the use of vulnerabilities to achieve access, there are distinct differences in both the technical and legal aspects.<sup>16</sup>

¶11 Section II first discusses how CALEA fit into the communications environment at the time, and then its disjunction with newly evolving communication systems. We then examine the reasons for and risks of extending CALEA to IP-based communications. The continued existence of vulnerabilities, fundamental to our proposal, is discussed in Section III. In Section IV, we discuss their use for wiretapping. Using exploits to enable wiretapping raises a number of troubling questions. As the Stuxnet cyberattack amply demonstrates, even carefully tailored exploits can extend past their intended target.<sup>17</sup> Therefore, law enforcement’s use of vulnerabilities requires careful consideration of how to limit the proliferation, which we discuss in Section V. Section VI considers whether law enforcement use of vulnerabilities should influence norms around vulnerability reporting. In Section VII, we discuss how to implement vulnerability reporting. We conclude our argument in Section VIII.

## II. CALEA: THE CHANGE IN WIRETAP ARCHITECTURE

¶12 The Communications Assistance for Law Enforcement Act (CALEA) was born of a certain time and certain place. It was a law created with the expectation of multiple, but relatively few, communications providers, and of a telephone network not substantially removed from the world of the Public Switched Telephone Network (PSTN) of the 1950s to 1980s. It was anticipated that both the technical and business structure of communications networks would remain centralized. The impact of the more fundamental changes that were percolating at the time of CALEA’s passage—IP-based communications and enormous numbers of services—were not anticipated at the time. In this section, we discuss the problems CALEA was intended to address and those it was

---

<sup>16</sup> “Remote search” is the capability to search the contents of a computer’s files via a surreptitious Internet connection. The investigator obtains access, presumably by hacking in, and runs assorted programs; in contrast, more usual searches involve seizing the computer and bringing it to a forensics lab. See, e.g., Susan W. Brenner, *Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force*, 81 MISS. L.J. 1229, available at [http://www.olemiss.edu/depts/ncjrl/pdf/2011%20Symposium/14-%20Brenner\\_FINAL.pdf](http://www.olemiss.edu/depts/ncjrl/pdf/2011%20Symposium/14-%20Brenner_FINAL.pdf); *EU to Search Out Cyber Criminals*, BBC NEWS, <http://news.bbc.co.uk/2/hi/technology/7758127.stm> (last updated Dec. 1, 2008).

<sup>17</sup> See generally Nicolas Falliere, Liam O Murchu, & Eric Chien, *W.32 Stuxnet Dossier*, SYMANTEC (Feb. 2011), [http://www.symantec.com/content/en/us/enterprise/media/security\\_response/whitepapers/w32\\_stuxnet\\_dossier.pdf](http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf) [hereinafter *Stuxnet Dossier*]. Stuxnet was apparently developed and launched by intelligence or cyberwarfare agencies; as such, its design is likely quite different from a law enforcement exploit.

not intended to address, briefly mention the security risks created by these solutions,<sup>18</sup> and the patchwork of solutions that have emerged to cover IP-based voice communications. We conclude by describing the impact of these changes on wiretapping and CALEA.

### A. History of CALEA

¶13

CALEA had its roots in the nascent switch to digital transport of voice over the phone network's local loops in the early 1990s. ISDN was touted as the next wave of telephony, since it could provide what was, for the time, very high-speed data over a switched line.<sup>19</sup> For all ISDN's advantages, however, it was not possible to tap ISDN lines with the traditional "two alligator clips and a tape recorder."<sup>20</sup> Furthermore, cellular telephony was growing rapidly; because the communication was wireless and mobile, cellular communications also could not be tapped with two alligator clips and a tape recorder. While specialized interception gear could have been developed, the FBI instead proposed in 1992 what was originally known as the Digital Telephony Bill, a standardized interface for wiretaps.<sup>21</sup> The bill was opposed by the telecommunications industry and civil-liberties organizations.<sup>22</sup> After considerable debate over the scope of coverage,<sup>23</sup> the current form of CALEA was passed, specifically excluding "information services."<sup>24</sup>

---

<sup>18</sup> Many countries around the world have similar laws. *See, e.g.*, Regulation of Investigatory Powers Act, 2000 c. 23, § 12 (Eng.), *available at* <http://www.legislation.gov.uk/ukpga/2000/23/part/I/chapter/I/crossheading/interception-capability-and-costs>. Our comments apply equally to all such laws.

<sup>19</sup> ISDN—Integrated Services Digital Network—was defined in Maurizio Dècina & Eric L. Scace, *CCITT Recommendations on the ISDN: A Review*, 4 IEEE J. ON SELECTED AREAS IN COMMS. 320, 320–25 (1986). In its most common form, it provided so-called 2B+D service: two 64 Kbps "bearer" channels, and a 16 Kbps data channel for signaling, e.g., call setup and teardown. *Id.* The two bearer channels could be combined into a single 128 Kbps link for pure data; this is more than twice as fast as any single-line analog phone modem can ever provide. For a variety of reasons, it never caught on in the United States as a common service.

<sup>20</sup> In the analog telephony era, wiretapping was very straightforward. It was almost as easy as plugging in a new extension phone, though some additional circuitry was needed or the target was not able to dial new calls or even hang up on a call. A law enforcement agent literally connected a pair of wires to the phone line going to the suspect's location; this connection could be done in the phone company's central office, at any point along the phone cable from the central office to the target, or, in the case of multiple occupancy buildings, in some utility space in the building. When the phone company started running digital signals to neighborhoods via "Subscriber Loop Carriers" (*see, e.g.*, Voyager[TNO], *The Subscriber Loop Carrier (Slick)*, PHRACK 8:52, Jan. 26, 1998 at article 11, <http://www.phrack.com/issues.html?issue=52&id=11>), the tap could be done in the same way, albeit from the neighborhood Remote Terminal onwards. Generally, a "loop extender" is employed to route the intercepted conversations back to a suitable facility. *See* Micah Sherr, Eric Cronin, Sandy Clark & Matt Blaze, *Signaling Vulnerabilities in Wiretapping Systems*, IEEE SECURITY & PRIVACY, Nov./Dec. 2005, at 13 vol. 3, no. 6 (2005): 13–25, <http://www.crypto.com/papers/wiretap.pdf>.

<sup>21</sup> *File 1—May '92 Version of FBI Digital Telephony Proposal*, COMPUTER UNDERGROUND DIG. (July 5, 1992), <http://cu-digest.org/CUDS4/cud429.txt>; *see also* WHITFIELD DIFFIE & SUSAN LANDAU, *PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION* 205–06 (Updated & Expanded ed. 2007).

<sup>22</sup> *See, e.g.*, Steven Levy, *Battle of the Clipper Chip*, N.Y. TIMES, June 12, 1994, <http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html>.

<sup>23</sup> In 1992, the FBI proposed legislation that would have "allowed the technical design mandates on any provider of any electronic communications, including the Internet." Corrected Petition for Rehearing En Banc at 12, *Am. Council on Educ. v FCC*, No. 15-0504 (D.C. Cir. July 28, 2006), *available at*

¶14 CALEA was intended to apply only to telephony. More precisely, CALEA was intended to apply only to “local exchange service,” i.e., local phone service but not long distance carriers.<sup>25</sup> Then-FBI Director Louis Freeh made clear in his 1994 Congressional testimony that the Internet was not covered:

Mr. FREEH. . . . We are really talking about phone-to-phone conversations which travel over a telecommunications network in whole or part. That is the arena of criminal opportunity that we are discussing.

Senator PRESSLER. What other portions of the information superhighway could people communicate with the new technology that there is not now a means of listening in or following?

Mr. FREEH. From what I understand, and again, I am probably the worst person in this room to answer the question, communications between private computers, PC-PC communications, not utilizing a telecommunications common net, would be one vast arena, the Internet system, many of the private communications systems which are evolving. Those we are not going to be on by the design of this legislation.

Senator PRESSLER. Are you seeking to be able to access those communications also in some other legislation?

Mr. FREEH. No, we are not. We are satisfied with this bill. I think it delimits the most important area and also makes for the consensus, which I think it pretty much has at this point.<sup>26</sup>

¶15 This consensus was reflected in the law, which defined a “telecommunications carrier” to include “a person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service and that it is in the public interest to deem such a person or entity to be a telecommunications carrier for purposes of this subchapter.”<sup>27</sup>

¶16 More recently, CALEA coverage has been extended to “last mile” service: the link between a residence or business and its ISP. Although controversial because of Freeh’s testimony and the exclusion of information services in CALEA, the FCC and the courts have held that this class of link is not included in the information services exclusion.<sup>28</sup>

---

<https://www.cdt.org/wiretap/calea/20060731calearehearing.pdf>. The proposal was “rejected out of hand”. *Id.* (quoting *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services: J. Hearings on H.R. 4922 and S. 2375 Before the Subcomm. on Tech. and the Law of the S. Comm. on the Judiciary & Subcomm. on Civil and Constitutional Rights of the H. Comm. on the Judiciary*, 103rd Cong. 49 (1994)).

<sup>24</sup> 47 U.S.C. § 1001(8)(C)(i) (2006).

<sup>25</sup> *Digital Telephony and Law Enforcement Access to Advanced Telecommunications Technologies and Services*, *supra* note 23, at 136.

<sup>26</sup> *Id.* at 202.

<sup>27</sup> See 47 U.S.C. § 1001(8)(B)(ii) (2006).

<sup>28</sup> *Am. Council on Educ. v. FCC*, 451 F.3d 226, 230 (D.C. Cir. 2006).

More precisely, the FCC made that ruling, and, relying on *Chevron* deference, the Court of Appeals upheld the FCC's ruling.<sup>29</sup>

¶17 Though important, this change to CALEA is of less concern to law enforcement than is the fate of the traditional telephone network. It is going away, and far faster than anyone had forecast. Already, more than 35% of American households do not have landline phone service, and about 16% more who have landlines never or almost never receive calls on them.<sup>30</sup> Indeed, the working assumption in the Federal Communications Commission (FCC) is that the PSTN will effectively cease to exist by 2018.<sup>31</sup>

### B. Wiretap Consequences of Splitting Services and Infrastructure

¶18 It might be tempting to say that the coming end of the PSTN vindicates the FBI's vision when it proposed CALEA. The actual situation, though, is far more complex; the decoupling of services from the physical link has destroyed the chokepoint at which CALEA could be applied. This does not appear to have been anticipated at the time of CALEA's passage.

¶19 A paradigmatic case in which the decoupling presents serious wiretapping problems is when communication occurs through use of Voice over Internet Protocol (VoIP). A VoIP phone provider can be located far from its subscribers; indeed, it could be in another, possibly unfriendly, country. Furthermore, the "signaling path"—the set of links that carry the call setup messages—can differ from the "voice path"—the links that carry the actual conversation.<sup>32</sup> (Tapping the last mile connection is likely fruitless, since VoIP connections are often encrypted.)

¶20 This is best explained by a diagram. Figure 1 shows a plausible setup for a VoIP call from Alice to Bob.<sup>33</sup> Alice's and Bob's phones are each connected to their own ISPs, Net 1 and Net 4. They each subscribe to their own VoIP provider, which in turn is connected to their ISPs. The signaling messages—that is, the messages used to set up the call, indicate ringing, etc.—go from Alice's phone, through her ISP to VoIP Provider 1's ISP, to her phone company. It then contacts VoIP Provider 2, via its ISP; VoIP Provider 2 sends a message through Net 4 to Bob's phone. The actual voice path, however, goes directly from Net 1 to Net 4; neither Net 2, Net 3, nor the VoIP providers even carry the actual conversation. As noted, any or all of the messages may be encrypted.

---

<sup>29</sup> See *id.* at 231 (citing *Chevron U.S.A. Inc. v. Natural Res. Def. Council, Inc.*, 467 U.S. 837, 842–43 (1984)).

<sup>30</sup> STEPHEN J. BLUMBERG & JULIAN V. LUKE, NAT'L CTR. FOR HEALTH STATISTICS, WIRELESS SUBSTITUTION: EARLY RELEASE OF ESTIMATES FROM THE NATIONAL HEALTH INTERVIEW SURVEY, JANUARY-JUNE 2012 1 (Dec. 2012), available at <http://www.cdc.gov/nchs/data/nhis/earlyrelease/wireless201212.pdf>.

<sup>31</sup> TECHNICAL ADVISORY COUNCIL, FEDERAL COMMS. COMMISSION, SUMMARY OF MEETING (Sept. 27, 2011), available at <http://transition.fcc.gov/oet/tac/tacdocs/tac-meeting-summary-9-27-11-final.docx>.

<sup>32</sup> See STEVEN BELLOVIN, MATT BLAZE, ERNEST BRICKELL, CLINTON BROOKS, VINTON CERF, WHITFIELD DIFFIE, SUSAN LANDAU, JON PETERSON & JOHN TREICHLER, SECURITY IMPLICATIONS OF APPLYING THE COMMUNICATIONS ASSISTANCE TO LAW ENFORCEMENT ACT TO VOICE OVER IP 2–7 (2006), available at <https://www.cs.columbia.edu/~smb/papers/CALEAVOIPreport.pdf> (demonstrating a VoIP network in Figure 1 on pg. 4).

<sup>33</sup> This figure is adapted from *id.* at 4.

¶21 In this setup, where can a tap be placed? On any of the ISPs? Law enforcement has no a priori information where Alice and Bob will be—their current IP addresses—prior to their setting up a call, so law enforcement cannot serve the ISPs with a wiretap order. To make matters worse, the ISPs have nothing to do with the VoIP call, nor can they read the encrypted traffic. How about at one of the VoIP providers? They do not see the voice traffic. And, of course, they may be in a different jurisdiction (for example, Skype was originally hosted in Luxembourg). This is a scenario that has no points amenable to a CALEA-like solution.

¶22 Other services are more complex still. Consider the new phone service being offered by Republic Wireless, which uses a combination of IP and PSTN networks to make a call. The service is intended to operate primarily over WiFi networks and the Internet; however, it can switch to Sprint's 3G cellular network as needed.<sup>34</sup> Where could a CALEA tap be placed? A tap could certainly be placed on the Internet-facing side of Republic's facilities,<sup>35</sup> but that would miss Sprint calls. Conversely, there could be one on Sprint's network, but that would miss calls made via VoIP. It is of course possible to place taps on both networks, but the protocols are very different. Since the ordinary signaling mechanisms are not used, special code would be needed to hand off not the call and the information necessary to carry out the tap.<sup>36</sup> Pen registers would be even more involved because the types of information easily recorded—phone numbers versus IP addresses—would vary.

¶23 Apart from reasonably straightforward (though structurally different) PSTN replacements, a large variety of other communications schemes have gained popularity. Email and text messages are two obvious examples, though even these pose challenges for law enforcement due to issues of personal jurisdiction and lack of real-time access to content. Skype is perhaps the most extreme case. Its architecture, which an FCC report calls “over the top,”<sup>37</sup> has no central switches. Even apart from questions of jurisdiction, there are *no* locations where a CALEA-style interface could be provided. Everything is done peer-to-peer; ordinary Skype users forward signaling traffic for each other.<sup>38</sup>

---

<sup>34</sup> Walt Mossberg, *For \$19, an Unlimited Phone Plan, Some Flaws*, WALL ST. J., Feb. 19, 2013, <http://allthingsd.com/20130219/for-19-an-unlimited-phone-plan-some-flaws/>.

<sup>35</sup> Tapping the customer's own Internet connection would not suffice, since the customer is likely to use multiple WiFi networks that such a tap would miss. Also, while Republic Wireless is a U.S. company, there is no reason why a similar service could not be offered by an offshore company over which U.S. courts have no jurisdiction.

<sup>36</sup> As of this writing, the Republic Wireless network cannot do handoffs of an in-progress call from a WiFi network to Sprint or vice-versa. According to Mossberg, *supra* note 34, that feature is planned for the near future.

<sup>37</sup> CRITICAL LEGACY TRANSITION WORKING GROUP, SUN-SETTING THE PSTN (2011), *available at* [http://transition.fcc.gov/oet/tac/tacdocs/meeting92711/Sun-Setting\\_the\\_PSTN\\_Paper\\_V03.docx](http://transition.fcc.gov/oet/tac/tacdocs/meeting92711/Sun-Setting_the_PSTN_Paper_V03.docx).

<sup>38</sup> It is unclear how true this still is. Skype has long used a “supernode,” a well-connected user computer that carries considerably more traffic. Of late, Microsoft—the current owner of Skype—has been deploying dedicated supernodes in its own data centers. *See* Dan Goodin, *Skype Replaces P2P Supernodes with Linux Boxes Hosted by Microsoft (Updated)*, ARS TECHNICA (May 1, 2012, 12:23 PM), <http://arstechnica.com/business/2012/05/skype-replaces-p2p-supernodes-with-linux-boxes-hosted-by-microsoft/>. There have been some allegations that the replacement was done precisely to permit surveillance. *See, e.g.*, John D. Sutter, *Can Skype 'Wiretap' Video Calls?*, CNN, <http://www.cnn.com/2012/07/24/tech/web/skype-surveillance> (last updated July 24, 2012, 4:30 PM). However, these are disputed by Mary Branscombe, who insists the changes in architecture are about “improving performance and not appropriating bandwidth.” *Forget the Conspiracy Theories: Skype's Supernodes Belong in the Cloud*, ZDNET (July 27, 2012, 1:52 PM), *available at*

Because of this, there are no trusted elements that could serve as wiretap nodes, at least for pen register orders. Furthermore, calls are always encrypted end-to-end.<sup>39</sup>

¶24

It is useful to contrast the Skype architecture with the conventional client-server architecture shown in Figure 1. In the conventional configuration, the VoIP providers run servers to which the individual phones—the clients—connect. These are architecturally different roles; when setting up calls, phones talk only to their associated servers and the servers talk to the clients and to each other. It is not possible for Alice’s phone to contact VoIP Provider 2 directly; they have no business relationship, and therefore cannot set up a direct network link.<sup>40</sup> In a peer-to-peer setup such as that used by Skype, there are *no* servers, i.e., no architecturally distinguished roles.<sup>41</sup> Rather, *every* computer or device running a Skype client can participate in the signaling. Alice’s phone (somehow) finds another Skype client and asks it to connect to Bob. This node finds another, which finds another, etc., until Bob’s phone is located.<sup>42</sup> At that point, Alice’s and Bob’s phones exchange signaling messages and set up the voice path. This voice path is in principle direct, though for various reasons, including the existence of firewalls, other Skype nodes may relay the (encrypted) voice packets. The lack of central servers, other than for user registration and enhanced services such as calling out to PSTN numbers, dramatically cuts the operational costs and allows Skype to offer free or extremely cheap phone calls.<sup>43</sup>

¶25

All that said, one of Snowden’s revelations was that the NSA can indeed intercept Skype calls.<sup>44</sup> No technical details have been disclosed; all we know is that the NSA can

<http://www.zdnet.com/forget-the-conspiracy-theories-skypes-supernodes-belong-in-the-cloud-700001720/>. The one-time principal architect of Skype, Matthew Kaufman, has explained that the change was done to accommodate the switch from always-on desktops to battery-powered mobile devices. See Zack Whittaker, *Skype Ditched Peer-to-Peer Supernodes for Scalability, not Surveillance*, ZDNET (June 24, 2013, 4:02 PM), <http://www.zdnet.com/skype-ditched-peer-to-peer-supernodes-for-scalability-not-surveillance-7000017215/>. Microsoft has applied for a patent on mechanisms for eavesdropping on VoIP networks, and some commentators have alleged that this technology will be incorporated into Skype. See, e.g., Jaikumar Vijayan, *Microsoft Seeks Patent for Spy Tech for Skype*, COMPUTERWORLD (June 28, 2011, 5:06 PM), [https://www.computerworld.com/s/article/9218002/Microsoft\\_seeks\\_patent\\_for\\_spy\\_tech\\_for\\_Skype](https://www.computerworld.com/s/article/9218002/Microsoft_seeks_patent_for_spy_tech_for_Skype).

<sup>39</sup> For a good, albeit dated—and paid for by Skype—review of the encryption architecture, see TOM BERSON, ANAGRAM LABS., *SKYPE SECURITY EVALUATION* (Oct. 18, 2005), <http://www.anagram.com/berson/abskyeval.html>.

<sup>40</sup> This is not a technical limitation per se; however, VoIP Provider 2 knows nothing of Alice’s phone, and hence is not willing to believe any assertions about its phone number, the person who uses it, etc. More importantly, because of the lack of a business relationship, it will not provide service to Alice’s phone since it will not be paid for its efforts.

<sup>41</sup> This is not strictly true. The Skype servers, however, are involved only in registering new users and providing them with cryptographic credentials. They are not involved in call setup, let alone being in the voice path. See *What Are P2P Communications?*, SKYPE, <https://support.skype.com/en/faq/fa10983/what-are-p2p-communications> (last visited Nov. 11, 2013).

<sup>42</sup> How the call eventually reaches Bob’s phone is a rather complex technical matter, and not relevant here. Let it suffice to say that Skype nodes regularly exchange enough navigational messages that it can be done.

<sup>43</sup> The lack of central servers was a deliberate architectural choice, designed to evade legal constraints. Architecturally, Skype was based on the Kazaa file-sharing network, which was in turn designed to operate without vulnerable nodes that could be targeted by copyright infringement lawsuits. For information about the history and technology of Skype, see generally Doug Aamoth, *A Brief History of Skype*, TIME (May 10, 2011), <http://techland.time.com/2011/05/10/a-brief-history-of-skype/>.

<sup>44</sup> See Glenn Greenwald, Ewen MacAskill, Laura Poitras, Spencer Ackerman & Dominic Rushe, *Microsoft Handed the NSA Access to Encrypted Messages*, THE GUARDIAN, July 11, 2013,

intercept audio and video, with complete metadata. It remains unclear if the solution is one that is usable by ordinary law enforcement, or if it relies on techniques (such as advanced cryptanalysis) that rely on the intelligence community's capabilities.<sup>45</sup>

¶26 Text messaging has also changed. Originally, it was a simple protocol for mobile phones. Recently, a number of variant implementations have been developed. Some provide a better experience in some fashion (for example, Apple's iMessage will send copies of inbound messages to all of a user's devices, including tablets and Mac computers as well as phones); others do things like provide phone-like text messaging for non-phone devices such as tablets.<sup>46</sup>

¶27 Non-traditional text messaging applications have already proven problematic. According to one report, attributed to a Drug Enforcement Administration memo, the encryption used by Apple's iMessage has already stymied wiretap orders.<sup>47</sup> There are even instant messaging applications designed not just to encrypt traffic, but to provide "repudiation," the ability to deny that you sent certain traffic.<sup>48</sup>

¶28 Further, many non-obvious communications mechanisms can serve for direct communications as well. In one well-known case, General David Petraeus and Paula Broadwell sent each other messages by creating and saving draft email messages in a shared Gmail account.<sup>49</sup> Additionally, many multiplayer games include text or even real-time voice communications between players; while nominally intended to lend realism to the game—soldiers in the same unit in action games can talk to each other and fighters on

---

<http://www.guardian.co.uk/world/2013/jul/11/microsoft-nsa-collaboration-user-data/print>.

<sup>45</sup> Microsoft claims that in 2012 it produced "no content" to law enforcement from Skype calls. See Brad Smith, *Microsoft Releases 2012 Law Enforcement Requests Report*, MICROSOFT ON THE ISSUES (Mar. 21, 2013, 6:00 AM), [https://blogs.technet.com/b/microsoft\\_on\\_the\\_issues/archive/2013/03/21/microsoft-releases-2012-law-enforcement-requests-report.aspx](https://blogs.technet.com/b/microsoft_on_the_issues/archive/2013/03/21/microsoft-releases-2012-law-enforcement-requests-report.aspx). The reports themselves are available at *Law Enforcement Requests Report*, MICROSOFT, <https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency/> (last visited Oct. 4, 2013).

<sup>46</sup> There are many such applications currently available and new ones are constantly appearing. See, e.g., Tanya Menoni, *6 Free iPhone & iPod Touch Texting Apps*, ABOUT.COM, <http://ipod.about.com/od/iphoneappsreviews/tp/4-Ways-To-Text-With-The-Ipod-Touch.htm> (last visited Sept. 21, 2013).

<sup>47</sup> See Declan McCullagh & Jennifer Van Grove, *Apple's iMessage Encryption Trips up Feds' Surveillance*, CNET NEWS (Apr. 4, 2013, 4:00 AM), [http://news.cnet.com/8301-13578\\_3-57577887-38/apples-imessage-encryption-trips-up-feds-surveillance/](http://news.cnet.com/8301-13578_3-57577887-38/apples-imessage-encryption-trips-up-feds-surveillance/). Because the design of the protocol has not been published, it has not been possible for outside experts to assess this claim. Some have asserted, based on certain externally visible characteristics (like the ability to do a password reset and still see old messages), that the messages must be stored unencrypted on Apple's servers. See, e.g., Julian Sanchez, *Untappable Apple or DEA Disinformation?*, CATO INSTITUTE (Apr. 4, 2013, 5:24 PM), <http://www.cato.org/blog/untappable-apple-or-dea-disinformation>. If that is true, a court order under the Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2006), would provide law enforcement with the content, albeit perhaps not in real-time.

<sup>48</sup> See Nikita Borisov, Ian Goldberg & Eric Brewer, *Off-the-Record Communication, or, Why Not to Use PGP*, PROC. 2004 ACM WORKSHOP ON PRIVACY ELECTRONIC SOC'Y 77, 77–78 (2004). Note that "repudiation" (derived from its more cryptographic common counterpart, "nonrepudiation") is used here as a computer scientist would use it—it refers to certain cryptographic properties: in terms of the encryption mechanisms used, it is not possible to show mathematically that a given person has sent certain messages. Concepts that a lawyer might rely on, e.g., circumstantial evidence or eyewitness testimony to the contrary, are not part of this mathematical model. Software to add repudiation to several IM programs is available at <https://otr.cypherpunks.ca/>.

<sup>49</sup> See Max Fisher, *Here's the E-Mail Trick Petraeus and Broadwell Used to Communicate*, WASH. POST, Nov. 12, 2012, <http://www.washingtonpost.com/blogs/worldviews/wp/2012/11/12/heres-the-e-mail-trick-petraeus-and-broadwell-used-to-communicate/>.

opposing sides can yell challenges or insults—such applications can also be used for surreptitious communications. Given that the Internet *is* a communications network, this raises the specter that *all* programs can be considered communications systems.

### C. *New Technologies: Going Dark or Going Bright?*

¶29 Collectively, the changes in telephony, the rise of new communications technology, and (to some extent) the increasing use of encryption, have been called the “Going Dark” problem because law enforcement has been unable to keep up with these changes and is losing access to criminals’ communications. Technology works both ways, however; others have rightly claimed that modern developments have actually *increased* the practical ability of law enforcement to monitor criminals’ behavior via assorted forms of metadata analysis; these analyses do not require warrants<sup>50</sup> So, how serious is the Going Dark problem? How has the balance changed?

¶30 A firm, quantitative answer to the former question is probably not possible. We cannot determine how many tap attempts would fail because law enforcement has said that it does not seek wiretap orders for calls it cannot intercept.<sup>51</sup> Furthermore, the situation is not static since both criminals and police adapt their tactics in response to each other’s capabilities and tactics. Consider cellular telephony. Under the Omnibus Crime Control and Safe Streets Act, the Administrative Office of the U.S. Courts (AO) reports annually on all Title III wiretaps.<sup>52</sup> The reports include the offense under investigation, the names of the prosecuting attorney and authorizing judge, the number of intercepts conducted and number of incriminating intercepts, the cost of the surveillance, etc.<sup>53</sup> In 2000, the report began listing how many wiretaps were of portable devices; in that year, they comprised 719 out of a total 1,190 Title III wiretaps.<sup>54</sup> By 2009, it was 2,276 out of 2,376, or 96%.<sup>55</sup> This, of course, mirrors the trend of society as a whole; as noted, a majority of Americans rely on mobile phones for most of their incoming calls.<sup>56</sup>

¶31 Reliance on mobile phones provides a partial answer to the question of gaining and losing capabilities as a result of modern communication systems. Because mobile phones are far more likely to capture the target’s conversations—rather than those of a spouse or business associate—mobile phone taps are more valuable than wireline taps. Furthermore, mobile data can include information on a person’s location, which means

---

<sup>50</sup> The claim is that the existence and availability of other information, such as location data, commercial data dossiers, and readily available contact information has given law enforcement far more than technology has taken away. *See, e.g.*, SUSAN LANDAU, SURVEILLANCE OR SECURITY: THE RISKS POSED BY NEW WIRETAPPING TECHNOLOGIES, 99–101 (2011), and Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 COLUM. SCI. & TECH. L. REV. 416, 463–64 (2012).

<sup>51</sup> Personal comments to Susan Landau; *see also Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*, *supra* note 2, at 12 (prepared statement of Valerie Caproni, General Counsel, Federal Bureau of Investigation).

<sup>52</sup> The reports are available at *Wiretap Reports Archive*, U.S. CTS., [http://www.uscourts.gov/Statistics/WiretapReports/WiretapReports\\_Archive.aspx](http://www.uscourts.gov/Statistics/WiretapReports/WiretapReports_Archive.aspx) (last visited Feb. 25, 2013).

<sup>53</sup> See the list of text and appendix tables in, for example, ADMIN. OFFICE OF THE U.S. COURTS, 2011 WIRETAP REPORT 3–4 (June 2012).

<sup>54</sup> Admin. Office of the U.S. Courts, 2000 Wiretap Report 30 (Apr. 2001).

<sup>55</sup> Admin. Office of the U.S. Courts, 2009 Wiretap Report 32 (Apr. 2010).

<sup>56</sup> *See* Blumberg & Luke, *supra* note 30.



that 96% of wiretapped communications provide law enforcement with extremely valuable location information. The same is true of many Internet connections, whether fixed or mobile.<sup>57</sup> In other words, the prevalence of immediate communications—texting, cellular calls, and the like—and centralized services—for example, Gmail and Facebook—has vastly simplified law enforcement’s ability to both track suspects and access their communications.

¶32 Another way to assess the overall risk of communications that law enforcement cannot monitor is to look at the net effect of prior threats: how much has the police’s ability to monitor communications been affected by prior technological changes, such as encryption? The issue has long been a concern, so much so that in 1993, the government announced the so-called “Clipper Chip”—an encryption device designed to enable the government to read otherwise encrypted traffic.<sup>58</sup> The AO wiretap reports now include data on how often encryption has been encountered.<sup>59</sup> The data are interesting. The total between 2001-2011 is eighty-seven; of these, only one was the subject of a federal wiretap order. Moreover, the AO noted that law enforcement was able to decrypt all of the wiretapped communications.<sup>60</sup>

¶33 There is not a lack of communications products that provide end-to-end encryption, such as RIM’s Blackberries, Skype, etc. While there are smart criminals who do use—

---

<sup>57</sup> A technology known as “IP geolocation” can be used to determine where an Internet user is located. It is frequently used to enforce geographic restrictions on access to content. *See, e.g., Terms of Use Agreement*, MLB.COM, [http://mlb.mlb.com/mlb/official\\_info/about\\_mlb\\_com/terms\\_of\\_use.jsp#4I](http://mlb.mlb.com/mlb/official_info/about_mlb_com/terms_of_use.jsp#4I) (last visited Sept. 24, 2013) (“Due to the foregoing blackout restrictions, you may be required to authorized MLBAM to access your location data . . . .”). While many IP geolocation services provide fairly coarse resolution, some companies have done a far better job of geolocation by combining IP address information with outside data, such as search queries, purchase delivery records, etc.

<sup>58</sup> *See* John Markoff, *Electronics Plan Aims to Balance Government Access with Privacy*, N.Y. TIMES, Apr. 16, 1993, <http://www.nytimes.com/1993/04/16/us/electronics-plan-aims-to-balance-government-access-with-privacy.html>; *see also* Matt Blaze, *Notes on Key Escrow Meeting with NSA*, RISKS DIG. (Feb. 8, 1994, 4:04 PM), <http://catless.ncl.ac.uk/Risks/15.48.html#subj1> (“They indicated that the thinking was not that criminals would use key escrowed crypto, but that they should not field a system that criminals could easily use against them. The existence of key escrow would deter them from using crypto in the first place. The FBI representative said that they expect to catch ‘~only the stupid criminals~’ through the escrow system.”).

<sup>59</sup> As a result of Public Law 106-197, since 2000 the AO has reported the annual total of state and federal wiretap orders encountering encryption. *See* Pub. L. No. 106-197, § 2, 114 Stat. 246 (codified at 18 U.S.C. § 2519(2)(b)(iv) (2006)).

<sup>60</sup> *See* ADMIN. OFFICE OF THE U.S. COURTS, 2001 WIRETAP REPORT 5 (May 2002) (reporting sixteen wiretaps encountering encryption in 2001); ADMIN. OFFICE OF THE U.S. COURTS, 2002 WIRETAP REPORT 5 (Apr. 2003) (reporting sixteen wiretaps encountering encryption in 2002 and an additional eighteen in 2001); ADMIN. OFFICE OF THE U.S. COURTS, 2003 WIRETAP REPORT 5 (Apr. 2004) (reporting one wiretap encountered encryption in 2003); ADMIN. OFFICE OF THE U.S. COURTS, 2004 WIRETAP REPORT 5 (Apr. 2005) (reporting two wiretaps encountered encryption in 2004); ADMIN. OFFICE OF THE U.S. COURTS, 2005 WIRETAP REPORT 5 (Apr. 2006) (reporting thirteen wiretaps encountered encryption in 2005); ADMIN. OFFICE OF THE U.S. COURTS, 2006 WIRETAP REPORT 5 (Apr. 2007) (reporting no wiretaps encountered encryption in 2006); ADMIN. OFFICE OF THE U.S. COURTS, 2007 WIRETAP REPORT 5 (Apr. 2008) (reporting no wiretaps encountered encryption in 2007); ADMIN. OFFICE OF THE U.S. COURTS, 2008 WIRETAP REPORT 5 (Apr. 2009) (reporting two wiretaps encountered encryption in 2008); ADMIN. OFFICE OF THE U.S. COURTS, 2009 WIRETAP REPORT 5 (Apr. 2010) (reporting one wiretap encountered encryption in 2009); ADMIN. OFFICE OF THE U.S. COURTS, 2010 WIRETAP REPORT 9 (reporting six wiretaps encountered encryption in 2010); ADMIN. OFFICE OF THE U.S. COURTS, 2011 WIRETAP REPORT 5 (June 2012) (reporting twelve wiretaps encountered encryption in 2011). All but one these were state wiretaps (the one federal wiretap that encountered encryption occurred in 2004).

and even build—their own encrypted communications networks,<sup>61</sup> the AO numbers demonstrate that criminals against whom Title III wiretaps are used typically do not do so. Instead, they tend to use simple solutions: Commercial Off-The-Shelf (COTS) equipment and communications in the cloud (e.g., Gmail and Facebook). Few use the peer-to-peer communication channels that pose problems for law enforcement wiretaps.<sup>62</sup> The implication for law enforcement use of vulnerabilities for performing Title III wiretaps is simple: law enforcement will not need to go that route very often.

¶34 Put another way, criminals are like other people: few use cutting edge or experimental devices to communicate. Instead, they stick with COTS products. If nothing else, COTS products are generally easier to use and work better, a definite advantage. Furthermore, understanding of the fine details of new technologies, such as encryption, is limited. The distinction between end-to-end encryption and client-to-server encryption is not understood by most people, criminals included. Similarly, the question of whether the encryption is going to the right party is often not even asked. Good software usually performs the proper checks,<sup>63</sup> but even production code has had serious errors.<sup>64</sup>

¶35 From this perspective, the most serious threat to legally authorized wiretapping is exemplified by the Skype architecture. Virtually all email services feature (at most) encryption from the client to the mail server; the messages reside in plaintext on the mail providers' disks.<sup>65</sup> By contrast, Skype provides transparent end-to-end encryption from the sender to the receiver; there is no middle man that sees the communication “in the clear.” Skype is gaining an increasing share of the international telephony market.<sup>66</sup> Even with Skype, however, investigators are not completely shut out. Though the content is

---

<sup>61</sup> See, e.g., Spencer Ackerman, *Radio Zeta: How Mexico's Drug Cartels Stay Networked*, WIRED (Dec. 27, 2011, 3:41 PM), <http://www.wired.com/dangerroom/2011/12/cartel-radio-mexico/>.

<sup>62</sup> See sources cited *supra* note 61.

<sup>63</sup> The best example is how web browsers use encryption. When a browser connects via HTTPS, the web server sends its “certificate” to the browser. A full explanation of certificates is out of scope here; what is important is that they contain a cryptographically protected association between the website's name and a unique cryptographic key. Browsers verify that the name of the website contacted actually appears in the certificate; thus, you will not end up with an encrypted connection to EvilHackerDudez.org when you are trying to log in to your bank.

<sup>64</sup> Generally speaking, encryption on the Internet requires use of a “Public Key Infrastructure”. See, e.g., RUSS HOUSLEY, TIM POLK, *PLANNING FOR PKI: BEST PRACTICES GUIDE FOR DEPLOYING PUBLIC KEY INFRASTRUCTURE* (2001). Web connections and many other sorts of traffic are protected using the “Secure Socket Layer”. See, e.g., ERIC RESCORLA, *SSL AND TLS: DESIGNING AND BUILDING SECURE SYSTEMS* (2001). For a discussion of applications that do some checks incorrectly, see Sascha Fahl, Marian Harbach, Thomas Muders, Matthew Smith, Lars Baumgärtner & Bernd Freisleben, *Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security*,” PROC. 2012 ACM CONF. ON COMPUTER AND COMM. SECURITY 50 (2012).

<sup>65</sup> Although probably technically feasible (though difficult, given the need to comply with industry standards), it is highly unlikely that providers, such as Google's Gmail and Microsoft's Hotmail, will switch to end-to-end encryption. There is little consumer demand, it is difficult, and Google at least relies on being able to scan messages in order to display appropriate ads. It cannot do so if the messages are encrypted.

<sup>66</sup> See *The Bell Tolls for Telcos?*, TELEGEOGRAPHY (Feb. 13, 2013), <http://www.telegeography.com/products/commsupdate/articles/2013/02/13/the-bell-tolls-for-telcos/> (“TeleGeography estimates that cross-border Skype-to-Skype voice and video traffic grew 44% in 2012 . . .”).

encrypted, Skype leaks the IP addresses of its users.<sup>67</sup> This provides the equivalent of pen register data and often location information as well.<sup>68</sup>

¶36 Technological changes will also play a role in law-enforcement's ability to wiretap. However, it is difficult at this point to make confident predictions about the future direction of technology. The two popular trends, cloud computing and peer-to-peer networking, have opposite effects on law enforcement's ability to monitor communications.

¶37 Cloud computing moves more and more storage and computation to distant, network-connected servers. Today's email scenario is an old but telling example: all of a target's email passes through easily monitored remote servers. These servers tend to have stringent backup regimens and log everything, out of operational necessity. Even deletion operations are less than permanent;<sup>69</sup> preservation of data is paramount, even under extreme circumstances.<sup>70</sup> In theory, cloud storage could be encrypted; in practice, because of users' desire to be able to search their email messages and the lack of customer demand, there has been little, if any, real-world deployment.<sup>71</sup> In fact, in order to better serve ads, the Facebook and Google business models rely on the cloud data being unencrypted.

¶38 The second trend, peer-to-peer, is decentralized, with no convenient points for wiretaps or content monitoring. Rather than clients and servers, computers, phones, and other gadgets talk to each other. Consider today's email architecture, where messages from Alice to Bob flow from her phone to her ISP's outbound mail server to Bob's ISP's inbound mail server to Bob's computer. Must it be done that way, or can Alice's phone talk directly to Bob's computers? Indeed, in some scenarios even ISPs disappear; in a technology known as "mesh networking," computers ask other peer computers to relay their traffic.<sup>72</sup> One very active area of development for mesh networks is car-to-car traffic for automotive safety and congestion control;<sup>73</sup> this could end up denying law

---

<sup>67</sup> See Joel Schectman, *Skype Knew of Security Flaw Since November 2010, Researchers Say*, WALL ST. J., May 1, 2012, <http://blogs.wsj.com/cio/2012/05/01/skype-knew-of-security-flaw-since-november-2010-researchers-say/>.

<sup>68</sup> See *supra* note 57.

<sup>69</sup> See, e.g., *Microsoft Services Agreement*, WINDOWS, <http://windows.microsoft.com/en-us/windows-live/microsoft-services-agreement> (last updated Aug. 27, 2012) (stating in Section 4.3: "please note that while content you have deleted or that is associated with a closed account may not be accessible to you, it may still remain on our systems for a period of time"). Other providers have similar provisions out of technical necessity.

<sup>70</sup> In 2010, a software problem caused thousands of Microsoft's Hotmail users to lose their entire mailboxes. Although it took several days, Microsoft was able to retrieve and restore the data from backup media. See Sebastian Anthony, *Hotmail Users Lose Entire Email Inboxes, Microsoft Restores Them 5 Days Later*, SWITCHED (Jan. 3, 2011, 6:50 AM), <http://downloadsquad.switched.com/2011/01/03/hotmail-users-lose-entire-email-inboxes-microsoft-restores-them/>.

<sup>71</sup> Encrypted storage and encrypted search are active research areas. However, except under special circumstances (e.g., a structured database, as opposed to email), encrypted remote search remains much more expensive than the plaintext equivalent and is likely to remain that way.

<sup>72</sup> See, e.g., Rafe Needleman, *Unbreakable: Mesh Networks are in your Smartphone's Future*, CNET (July 13, 2013, 5:00 AM), [http://www.cnet.com/8301-30976\\_1-57471447-10348864/unbreakable-mesh-networks-are-in-your-smartphones-future/](http://www.cnet.com/8301-30976_1-57471447-10348864/unbreakable-mesh-networks-are-in-your-smartphones-future/).

<sup>73</sup> See Jon Brodtkin, *Wireless Mesh Networks at 65MPH—Linking Cars to Prevent Crashes*, ARS TECHNICA (Jan. 9, 2013, 6:50 PM), <http://arstechnica.com/information-technology/2013/01/wireless-mesh-networks-at-65mph-linking-cars-to-prevent-crashes/>.

enforcement access to location data from cellular networks, because the phones would be talking to other phones in a peer-to-peer fashion rather than registering with phone company-run cell towers.

¶39 In a cloud world, monitoring will be easier; in a peer-to-peer world, it will be harder. It is quite possible that both trends will continue, with different applications and different markets opting for one solution over the other.

#### D. *The TPWG's Tracking Preferences Expression Standard*

¶40 CALEA II, the extension of CALEA to cover all communications applications, poses three serious problems: (1) it hinders innovation by restricting communications application developers to certain topological and trust models, (2) it imposes a financial tax on software, and (3) it creates security holes (and hence increases the risk of computer crime, cyberepionage, and cyberterrorism). This last point seems to be mentioned least in debates, although arguably it is the most important since it cannot be addressed by perfect (or at least very, very good) software development practices, reuse of standard CALEA compliance libraries, or both.

¶41 An implicit assumption behind CALEA-style laws is that there is a “good” place where intercepts can take place. Such a place would be run by trustworthy people who are not implicated in the investigation,<sup>74</sup> and be located where the tap cannot be detected. More or less of necessity, this translates to relying on a centralized facility, preferably one run by a large, accountable company. This worked well for the telephone taps, where all lines were connected to a phone switch run by a conventional phone company. By contrast, consider a Skype-like architecture with transmissions over a mesh network. There are *no* large companies involved in either the call setup or data paths; rather, both use effectively random links. Furthermore, there may be little or no logging present; not only is the path used for one call probably not the path used for another, there will be no logs to show what paths were used. This means little or no accountability for any parties who leak information, and no assurance whatsoever that anyone will be able to complete the tap.

¶42 The fact that a peer-to-peer service is not facilities-based—it does not rely on provider-owned equipment—also means there may be no parties to whom the law applies. For example, CALEA requires that “a telecommunications carrier shall ensure that its equipment, facilities, or services . . . enable[e] the government . . . to intercept . . . all wire and electronic communications carried by the carrier . . . concurrently with their transmission to or from the subscriber’s equipment.”<sup>75</sup> Based on the definition of telecommunications carrier provided in the statute, however, there are no carriers in some peer-to-peer architectures: “The term ‘telecommunications carrier’, means a person or entity engaged in the transmission or switching of wire or electronic communications as a

---

<sup>74</sup> 18 U.S.C. § 2511(2)(a)(ii) (2006) (“No provider of wire or electronic communication service, officer, employee, or agent thereof . . . shall disclose the existence of any interception or surveillance or the device used to accomplish the interception or surveillance with respect to which the person has been furnished a court order or certification under this chapter . . . . Any such disclosure, shall render such person liable for the civil damages provided for in section 2520.”) Damages after the fact are one thing, but law enforcement would much rather the tap were not disclosed in the first place.

<sup>75</sup> 47 U.S.C. § 1002(a) (2006).

common carrier for hire . . .”<sup>76</sup> or “a person or entity engaged in providing wire or electronic communication switching or transmission service to the extent that the Commission finds that such service is a replacement for a substantial portion of the local telephone exchange service.”<sup>77</sup> In a peer-to-peer network, there is no such thing as “local” service; a “peer” need not be geographically close to any of the parties. Similarly, there may be no “manufacturer of telecommunications transmission or switching equipment” who can be compelled to “make available to the telecommunications carriers using its equipment, facilities, or services such features or modifications as are necessary to permit such carriers to comply with the capability requirements”;<sup>78</sup> the peer nodes and any commercial entities involved in the service operation (and there need not be any) may be located outside of U.S. jurisdiction.<sup>79</sup>

¶43 To sum up, the laws assume a trustworthy, disinterested intermediary within the court’s jurisdiction. But as the net moves towards a more decentralized architecture, such third parties simply do not exist. Current technological trends pose a serious (and probably insurmountable) philosophical challenge to CALEA-style laws.

¶44 If CALEA were to be extended to cover IP-based communications, the law would have to specify which part of the service is responsible for supplying wiretap capability. As noted earlier, peer-to-peer networking is one plausible path for the technical future. Imposing requirements that effectively block this approach would have a very serious effect on innovation. Peer-to-peer communications have enabled some important applications such as BitTorrent, which is used by NASA for sharing satellite images, by various computer companies for sharing large files (e.g., open source operating systems), by gaming companies for sharing updates, and even by content providers such as CBS and Warner Bros. for delivering programming.<sup>80</sup>

¶45 There is a second burden on innovation: the extra cost, both in development effort and development time, to include wiretap interfaces in early versions of software is prohibitive. At first blush, CALEA compliance seems simple since the only information that is needed is dialed-out and dialing-in phone numbers and voice. At that level, it is simple; nevertheless, the document defining the standard interface to a CALEA-compatible switch is more than 200 pages long.<sup>81</sup> Imagine, then, the standards necessary to cover interception of email, web pages, social networking status updates, instant messaging (for which there are several incompatible protocols), images, video downloads, video calls, video conference calls, file transfer layered on top of any of

<sup>76</sup> *Id.* § 1001(8)(A).

<sup>77</sup> *Id.* § 1001(8)(B)(ii).

<sup>78</sup> *Id.* § 1005(b).

<sup>79</sup> A service without any operators does not imply that no one profits. The original KaZaA filesharing service was ad-supported. See Ryan Naraine, *Spyware Trail Leads to Kazaa, Big Advertisers*, EWEEK (Mar. 21, 2006), <http://www.eweek.com/c/a/Security/Spyware-Trail-Leads-to-Kazaa-Big-Advertisers/>; see also *Universal Music Australia Pty Ltd. v. Sharman License Holdings Ltd.* (2005) 65 IPR 289 (Austl.); BRIAN BASKIN ET AL., *COMBATING SPYWARE IN THE ENTERPRISE* 9–11 (Tony Piltzecker et al. eds. 2006). It is unreasonable and probably infeasible to impose wiretap requirements on advertisers because the chain of indirection from the software developer to the advertisers is too long and tenuous. See, e.g., Kate Kaye, *The Purchase-to-Ad Data Trail: From Your Wallet to the World*, AD AGE (Mar. 18, 2013), <http://adage.com/article/dataworks/purchase-targeted-ads-data-s/240300/>.

<sup>80</sup> See, e.g., Brad King, *Warner Bros. to Distribute Films Using Bit Torrent*, MIT TECH. REV. (May 9, 2006), <http://www.technologyreview.com/view/405794/warner-bros-to-distribute-films-using-bit-torrent/>.

<sup>81</sup> See TELECOMMS. INDUS/ ASS’N, TR-45 LAWFULLY AUTHORIZED ELECTRONIC SURVEILLANCE J-STD-025 REV. A (May 31, 2000), available at <http://cryptome.org/esp/TR45-jstd025a.pdf>.

these, games that have voice or instant messaging functions included, and more. It is simply not a feasible approach. Nor are these improbable uses of the Internet; all of them are used very regularly by millions of people.

¶46 Applying CALEA to Internet applications and infrastructure will be a “tax” on software developers. The much lower barriers to entry (relative to traditional telephone networks currently covered by CALEA) provided by the open architecture of the Internet have bred many startups. These are small and agile; they are often the proverbial “two guys in a garage.” Many will fail; even the eventual successes often start slowly. Regardless, they are essential to the Internet’s success. Skype started small, yet it is now one of the largest international phone carriers.<sup>82</sup> Another example is Facebook, which was started by an undergraduate in his dorm room. Indeed, the Web began as an information distribution system at a European physics lab.<sup>83</sup> It is hard to say at what point an experiment has become large enough to be a “service” worthy of being wiretap-friendly; it is clear, though, that requiring such functionality to be built in from the start is a non-trivial economic burden and a brake on innovation. By contrast, the PSTN is primarily composed of large, established companies who buy essentially all of their equipment from other large, established companies.<sup>84</sup>

¶47 The most serious problem with CALEA, however, is that it has created a new class of vulnerabilities. By definition, a wiretap interface is a security hole because it allows an outside party to listen to what is normally a private conversation. It is supposed to be controlled, in that only authorized parties should have access. Restricting access to such facilities is far more difficult than it would appear; the history of such mechanisms is not encouraging.

¶48 The risks are not theoretical. In the 2004 to 2005 “Athens Affair,” new code was injected into the phone switch that used the lawful intercept mechanisms to eavesdrop on about 100 mobile phones, including the Prime Minister’s.<sup>85</sup> In a similar but less publicized incident in Italy between 1996 and 2006, about 6,000 people were the target of improper wiretaps, apparently due to corrupt insiders who sought financial gain. Again, the lawful intercept mechanism was abused.<sup>86</sup>

---

<sup>82</sup> See *supra* note 66.

<sup>83</sup> See *From a 1997 Hand-Out for the General Public*, TEN YEARS PUB. DOMAIN FOR THE ORIGINAL WEB SOFTWARE, <http://tenyears-www.web.cern.ch/tenyears-www/Story/WelcomeStory.html> (last visited Nov. 12, 2013).

<sup>84</sup> Even for such companies, the expense of adding CALEA facilities was non-trivial. The statute, 47 U.S.C. §§ 1007–1009 (2006), authorized \$500 million “to pay telecommunications carriers for all reasonable costs directly associated with the modifications performed by carriers in connection with equipment, facilities, and services installed or deployed on or before January 1, 1995, to establish the capabilities necessary to comply with section 1002 of this title.” The funding was approved in the Omnibus Consolidated Appropriations Act, which provided for funding through a combination of money supplied by various intelligence agencies and \$60 million in direct funding. Omnibus Consolidated Appropriations Act, Pub. L. No. 104-208, 110 Stat. 3009 (1996). An additional \$12 million was provided through unspent Department of Justice funds. More than 95% of the money was actually spent; about \$40 million was rescinded by Congress in 2007. See U.S. DEP’T OF JUSTICE OFFICE OF INSPECTOR GEN., IMPLEMENTATION OF THE COMMUNICATIONS ASSISTANCE FOR LAW ENFORCEMENT ACT BY THE FEDERAL BUREAU OF INVESTIGATION ii–iii (Mar. 2008), available at <http://www.justice.gov/oig/reports/FBI/a0820/final.pdf>.

<sup>85</sup> See Prevelakis & Spinellis, *supra* note 4.

<sup>86</sup> See Piero Colaprico, Giuseppe d’Avanzo & Emilio Randacio, ‘Da Telecom Dossier sui Ds’ Mancini Parla dei Politici, LA REPUBBLICA (Jan. 26, 2007),

¶49 The U.S. is at risk, too. Phone switches are already large, extremely complex computer systems;<sup>87</sup> as such, they are *inherently* at risk. An NSA evaluation of CALEA-compliant phone switches found vulnerabilities in every single one examined.<sup>88</sup> It is not known publicly if any American phone switches have been penetrated; however, news reports do suggest foreign interest in American use of surveillance technology to determine who America’s surveillance targets are.<sup>89</sup>

¶50 There is one more aspect of security that has to be taken into account: who the enemies are. As has been widely reported in the press, various countries have created or are creating cyberespionage and cyberwarfare units.<sup>90</sup> These are highly skilled and well-equipped groups, easily capable of finding and exploiting subtle flaws in systems. To use an easy analogy, comparing the capabilities of such units to those of garden-variety hackers is like comparing the fighting power of modern infantrymen to that of a comparable-sized group of drug gang members. When considering the security of any Internet-connected systems that might attract the hostile gaze of foreign powers, this must be taken into account.

¶51 Communications systems fall into this category and have done so for many, many years. Even apart from their purely military significance, American economic interests have long been targeted by other nations. For example, in the early 1970s the Soviets reportedly used high-tech electronic eavesdropping devices to listen to the phone calls of American grain negotiators.<sup>91</sup> These days the attempts at economic espionage come not

---

<http://www.repubblica.it/2006/12/sezioni/cronaca/sismi-mancini-8/dossier-ds/dossier-ds.html>.

<sup>87</sup> W. Keister, R. W. Ketchledge & H. E. Vaughan, *No. 1 ESS: System Organization and Objectives*, 43 BELL SYS. TECHNICAL J. 1831, 1832 (1964) (calling the development of the 1ESS switch “the largest development project ever undertaken by Bell Laboratories for the Bell System.”); Ben Chelf, *Code Complexity for Embedded Software Makers Sure Has Changed*, EMBEDDED (Jan. 22, 2009), <http://www.embedded.com/electronics-blogs/industry-comment/4026959/Code-complexity-for-embedded-software-makers-sure-has-changed> (speaking of “extreme software development projects (e.g., AT&T’s phone switch)”); BRUCE STERLING, *THE HACKER CRACKDOWN: LAW AND DISORDER ON THE ELETRONIC FRONTIER* 37 (1992) (noting that the System 7 “signal transfer point”—a minor piece of phone switching equipment—is comprised of 10 million lines of source code). The best references that discuss the complexity phone switch software are proprietary documents (for example, 64 AT&T TECHNICAL J., no. 6, part 2, a special issue devoted to the 5ESS phone switch). One of the authors of this paper worked in the software engineering research department of the AT&T 5ESS phone switch development organization and saw the complexity first-hand.

<sup>88</sup> See Susan Landau, *The Large Immortal Machine and the Ticking Time Bomb*, 11 J. TELECOMM. & HIGH TECH. L. 1 (2013).

<sup>89</sup> See Kenneth Corbin, *‘Aurora’ Cyber Attackers were Really Running Counter-Intelligence*, CIO (Apr. 22, 2013), [http://www.cio.com/article/732122/\\_Aurora\\_Cyber\\_Attackers\\_Were\\_Really\\_Running\\_Counter\\_Intelligenc\\_e?taxonomyId=3089](http://www.cio.com/article/732122/_Aurora_Cyber_Attackers_Were_Really_Running_Counter_Intelligenc_e?taxonomyId=3089).

<sup>90</sup> For a discussion of exploits sponsored by the Chinese government, see MANDIANT, *APT1: EXPOSING ONE OF CHINA’S CYBER ESPIONAGE UNITS*, available at [http://intelreport.mandiant.com/Mandiant\\_APT1\\_Report.pdf](http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf) (last viewed Mar. 31, 2013) and David Sanger, David Barboza & Nicole Perloth, *Chinese Army Unit is Seen as Tied to Hacking Against U.S.*, N.Y. TIMES, Feb. 18, 2013, <http://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html>. For a discussion of exploits being conducted by the Israeli government, see, for example, William Broad, John Markoff & David Sanger, *Israeli Test on Worm is Considered Crucial in Iran Nuclear Delay*, N.Y. TIMES, Jan. 15, 2011, <http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html>. These are just two examples of many such efforts.

<sup>91</sup> DAVID KAHN, *KAHN ON CODES: SECRETS OF THE NEW CRYPTOLOGY* 193 (1983).

just from Russia, but also from China, France, Germany, Israel, Japan, South Korea, India, Indonesia, and Iran.<sup>92</sup>

¶52 In 2000, the Internet Engineering Task Force, the engineering group that develops Internet communications standards through its “Requests for Comment” (RFCs) documents, concluded that “adding a requirement for wiretapping will make affected protocol designs considerably more complex. Experience has shown that complexity almost inevitably jeopardizes the security of communications . . . ; there are also obvious risks raised by having to protect the access to the wiretap. This is in conflict with the goal of freedom from security loopholes.”<sup>93</sup> The security vulnerabilities that a wiretap introduces into a communications system are a serious problem, yet the problem apparently gets little attention from law enforcement in its efforts to expand CALEA to IP-based communications.

---

<sup>92</sup> Information on France, Germany, Israel, Japan, and South Korea can be found in INTERAGENCY OPSEC SUPPORT STAFF,

INTELLIGENCE THREAT HANDBOOK 5-5, 5-6 (1996), while information on China, India, Indonesia, and Iran can be found in OFFICE OF THE NAT’L COUNTERINTELLIGENCE EXEC., ANNUAL REPORT TO THE CONGRESS ON FOREIGN ECONOMIC COLLECTION AND INDUSTRIAL ESPIONAGE, FY07 2, 9–13 (Sept. 10, 2008), *available at* [http://www.ncix.gov/publications/reports/fecie\\_all/fecie\\_2007/FECIE\\_2007.pdf](http://www.ncix.gov/publications/reports/fecie_all/fecie_2007/FECIE_2007.pdf). The US has a policy of not conducting economic espionage; in response to the recent NSA leaks, this was recently stated quite explicitly: “It is not an authorized foreign intelligence or counterintelligence purpose to collect such information to afford a competitive advantage to U.S. companies and U.S. business sectors commercially.” A footnote goes on to say, “Certain economic purposes, such as identifying trade or sanctions violations or government influence or direction, shall not constitute competitive advantage.” Directive on Signal Intelligence Activity, 2014 DAILY COMP. PRES. DOC. 31 (Jan. 17, 2014).

<sup>93</sup> NETWORK WORKING GRP., IETF POLICY ON WIRETAPPING 2 (May 2000), *available at* <http://tools.ietf.org/html/rfc2804>. One of the authors of this paper was on the Internet Architecture Board at the time and helped write the document.



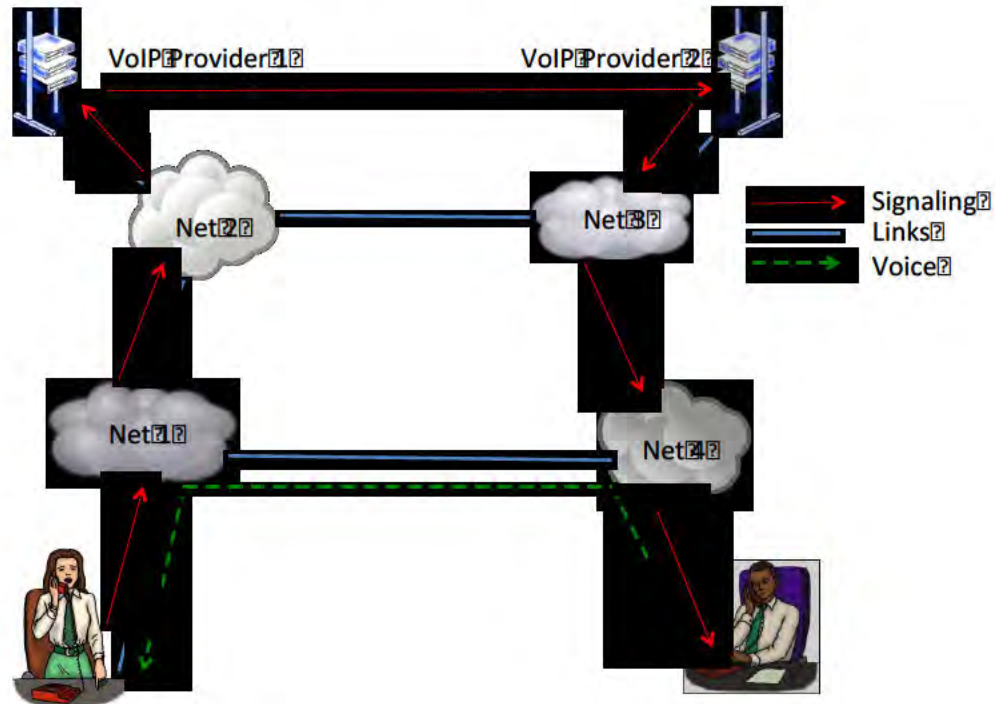


Figure 1: A Voice over IP (VoIP), showing physical links, the signaling path, and the voice path.

### III. THE VULNERABILITY OPTION

This section turns from the discussion of default DNT and the TPE bespoke standard to a broader discussion about automation and privacy. It makes two arguments. First, it argues that substantive theories of privacy must be considered especially suspect when their implementation actively increases the transaction costs involved in protecting privacy.<sup>94</sup> Second, it asserts that only automated features can sufficiently reduce consumer privacy transaction costs such that one might assess the contours of a market for privacy platforms. It concludes that advertising industry advocates do not embrace free-market principles, but rather seek to prevent products with innovative privacy features like default DNT from reaching the market.

<sup>94</sup> See McDonald & Cranor, *supra* note 73. (“Privacy policies should help reduce information asymmetries because companies share information with their customers . . . [but] if the cost for reading privacy policies is too high, people are unlikely to read policies.”); see also Jeff Sovern, *Toward a New Model of Consumer Protection: The Problem of Inflated Transaction Costs*, 47 WM. & MARY L. REV. 1635, 1637 (2006) (“In many circumstances, businesses benefit by increasing consumer transaction costs to the detriment of consumers . . . [S]ome practices are profitable largely because they inflate consumer transaction costs . . . [F]irms increase consumer transaction costs because doing so enriches them.”).

### A. Definition of Terms

¶54

We need to define a few commonly used technical terms in order to present the mechanics of employing a vulnerability for accessing a target system.<sup>95</sup>

**Vulnerability:** 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. Vulnerabilities can be bugs (defects) in the code, such as a “buffer overflow”<sup>96</sup> or a “use-after-free instance,”<sup>97</sup> or misconfigurations, such as not changing a default password or running open, unused services.<sup>98</sup> Another common type of vulnerability results from not correctly limiting input text (this is also known as not sanitizing input), e.g., “SQL injection.”<sup>99</sup> Alternatively, a vulnerability can be as simple as using a birth date of a loved one as a password. A vulnerability can be **exploited** by an attacker. A special instance of vulnerability is the:

**Zero-day** (or 0-day vulnerability): A zero-day is a vulnerability discovered and exploited prior to public awareness or disclosure to the vendor. Zero-days are frequently sold in the vulnerabilities market. The vendor and the public often only become aware of a zero-day after a system compromise.

---

<sup>95</sup> Many of these terms are defined in R. SHIREY, INTERNET SECURITY GLOSSARY, VERSION 2 (Aug. 2007), available at <http://tools.ietf.org/pdf/rfc4949.pdf>. Others are common terminology in the hacker and security communities, but have yet to be defined in any authoritative work.

<sup>96</sup> A buffer overflow is caused by a program accepting more input than memory has been allocated for. Conceptually, imagine a clerk writing down someone’s name, but the name as given is so long that it doesn’t fit in the box on a form and spills over into the “Official Use Only” section of the form. A buffer overflow error was a central part of the Internet Worm of 1988, which resulted in the first case ever brought under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2006). See *United States v. Morris*, 928 F.2d 504 (2nd Cir. 1991). In some programming languages, e.g., Java, such overflows are detected automatically by the system; programmers using older languages, such as C, can use safe programming techniques that avoid the problem. A variety of tools can be used to detect potentially unsafe areas of programs. These have become increasingly common in the last 10 years, to very good effect.

<sup>97</sup> Programs can request storage space, then release (“free”) it when they are done; after that, the space is available for other uses. A use-after-free bug involves carefully crafted accesses to memory no longer allocated for its original purpose; if some other section of the program is now reusing that storage, this section of the program may be confused by the improper reuse.

<sup>98</sup> A service is a mechanism by which programs listen for and act on requests from other programs; often, these services are available to any other computer that can contact this one via the Internet. The best analogy is to room numbers in a building. The building itself has a single address (the computer analog is the IP address), but the mailroom is in room 25, the information counter is in room 80, and so on. When one computer tries to contact another, it must specify the second computer’s address (i.e., the building) and the service (i.e., the room number). Secure computer systems generally “listen” on very few ports, since each one represents a potential external vulnerability. (To continue our analogy, a building that does not need a mailroom will not have one that might somehow be abused.) Suppose, for example, that a computer that is not intended to act as a web server is in fact running web server code. A flaw in that web server can result in system penetration; the simplest fix is to turn off the web service since it is unneeded on that computer. See *CERT Advisory CA-2001-19 “Code Red” Worm Exploiting Buffer Overflow in IIS Indexing Service DLL*, CERT (July 19, 2001), available at <http://www.cert.org/advisories/CA-2001-19.html>, for an example of problems caused by open, unneeded services.

<sup>99</sup> In some contexts, parts of the input to a program can be interpreted as programming commands rather than as data. SQL injection attacks—in variant forms, they date back to at least the 1970s—occur when programmers do not filter input properly to delete such commands.

**Exploit:** An exploit is the means used to gain unauthorized access to a system. This can be a software program, or a set of commands or actions. Exploits are usually classified by the vulnerability of which they take advantage and whether they require local (hands-on) access to the target system or can be executed remotely or through a web page or email message (drive-by).<sup>100</sup> The type of result obtained from running the exploit depends on the **payload** (rootkit, key-logger, etc.). The payload is chosen when the exploit is run or **launched**. An exploit demonstrates the use of the vulnerability in actual practice.

**Payload:** The payload of an exploit is the code that is executed on the target system giving the attacker the desired access. Payloads can be single action, such as surreptitiously creating a new user account on the system that allows future access, or multi action, such as opening a remote connection to the attacker's server and executing a stream of commands. The payload generally must be customized to the specific system architecture of the target.

**Dropper:** A dropper is a malware component or malicious program that installs the payload on the target system. A dropper can be single stage, a program that executes on the target system as a direct result of a successful exploit and carries a hidden instance of the payload, or it can be multi-stage, executing on the target system, but downloading files (including the payload) from a remote server.

**Man-in-the-Middle attack:** A Man-in-the-Middle attack is a method of gaining access to target information in which an active attacker interrupts the connection between the target and another resource and surreptitiously inserts itself as an intermediary. This is typically done between a target and a trusted resource, such as a bank or email server. To the target the attacker pretends to be the bank, while to the bank the attacker pretends to be the target. Any authentication credentials required (e.g., passwords or certificates) are **spoofed** by the attacker, so that each side believes they are communicating with the other. But because all communications are being transmitted through the attacker, the attacker is able to read and modify any messages it wishes to.

**Spoofing:** In the context of network security, a spoofing attack is a situation in which one person or program successfully masquerades as another by falsifying data and thereby gaining an illegitimate advantage.<sup>101</sup>

### B. *How Vulnerabilities Help*

¶55

Our claim is that pre-existing vulnerabilities in software make extending CALEA unnecessary.<sup>102</sup> To understand the scenarios in which these vulnerabilities might be used, it is necessary to give a simplified description of the structure of modern computer

---

<sup>100</sup> A drive-by download is an attack perpetrated simply visiting a malicious or infected website. No further action by the user is necessary for the attack to succeed. Such attacks *always* result from underlying flaws in the web browser.

<sup>101</sup> SHIREY, *supra* note 95, at 187, 290 (defining “spoofing” as equivalent to “masquerade attack,” which in turn is defined as “[a] type of threat action whereby an unauthorized entity gains access to a system or performs a malicious act by illegitimately posing as an authorized entity”).

<sup>102</sup> Some of this material appeared in different form in Bellovin, Blaze, Clark & Landau, *supra* note 5.

operating systems.<sup>103</sup> Systems are described in terms of “layers”; each layer provides some services to the layer above it, and requests services of the layer below it. Often, a combination of hardware and software enforces the boundary between layers, ensuring that only certain requests can be made of the lower layer.

¶156 The lowest layer we will mention is the hardware: CPU chips such as Intel’s Pentium series, devices such as network interfaces and hard drives, USB ports, etc. For our purposes, we will assume that this layer is error-free and secure. While not strictly true, attacks at this level are generally more feasible for the greater capabilities of national security purposes than for law enforcement.<sup>104</sup>

¶157 The next layer is generally called the “kernel.” The kernel protects itself against corruption (with aid from the hardware), and is also the only component that directly communicates with external hardware such as the network. When a program needs to read or write from the network or a disk drive, it cannot do so directly; instead, it asks the kernel to perform the action for it. A consequence of this is that the kernel has to enforce “file permissions”: which users of the computer own which file, who can read or write them, etc. That in turn implies that there must be some strong separation between programs run by different users; again, the kernel enforces this.

¶158 The last layer of interest is the “user level” or “application level.” Virtually all programs of interest—web browsers, mailers, document editors and viewers, and so on—run at user level. Running programs are typically associated with some user. The user may be a physical individual; however, all modern systems have a large number of helper processes, sometimes known as “daemons,” running as some flavor of system pseudo-user. These handle such applications as the audio system, indexing files, insertion of USB devices, and more. A quick check of a modern Apple Mac showed no fewer than 10 different pseudo-users active on the machine.

¶159 All modern operating systems have a feature known as a “sandbox.” A sandbox is a way of enforcing security by allowing a program to run with fewer privileges than the user who invoked it.<sup>105</sup> Sandboxes are frequently used for programs perceived as exceptionally vulnerable to security holes, such as PDF viewers and web browsers.

¶160 Vulnerabilities—and hence exploits of use to law enforcement—can occur at any layer, but the capabilities available to the exploit are different at different layers. While we defer details until Section IV, we note that for an exploit to work, more code is needed than just something that targets the vulnerability. In particular, to perform a wiretap—that is, to acquire the contents of a communication—the actual data sent or received has to be captured. This can be done in a particular application (e.g., Skype or a game with a voice communications feature), or it could be done at kernel level by tampering with a “device driver,”<sup>106</sup> in which case data from any application could be captured. A kernel exploit is well-positioned to modify device drivers; however, for

---

<sup>103</sup> These days, smartphones are built the same way, so there is no need to discuss them separately.

<sup>104</sup> We will not discuss attacks like eavesdropping on encrypted WiFi signals. In principle, though, there might be exploitable vulnerabilities in the target’s WiFi access point or router. These devices, though, are just computers and can be hacked like any other computers.

<sup>105</sup> See SHIREY, *supra* note 95.

<sup>106</sup> A *device driver* is a special part of the kernel that communicates with input/output devices such as disks, audio ports, network interfaces, etc. See, e.g., ANDREW S. TANENBAUM AND ALBERT S. WOODHULL, OPERATING SYSTEMS DESIGN AND IMPLEMENTATION 231–33 (3d ed. 2006).

complex technical reasons such an attack would find it more difficult to read and write files, export captured data via the network, etc.<sup>107</sup>

¶161 Most initial penetrations take place at application level.<sup>108</sup> The mechanisms vary widely, including infected attachments in email, malware on web pages, poor implementations of network protocols, and users downloading and voluntarily executing booby-trapped programs under a misapprehension as to the programs' purpose, provenance, and good intent.<sup>109</sup> The results are the same: some program the user had not intended is being run with the user's file access rights.

¶162 Under certain circumstances, this insecurity is sufficient for law enforcement purposes. For example, it generally provides adequate means for intercepting email. It may also suffice for looking at the transcript files kept by some instant messaging programs.

¶163 On the other hand, if the program penetrated is not used for the actual communications of interest, these application-level exploits alone will not suffice. Consider that on most modern platforms, users—and hence the programs they run—do not have the ability to tamper with the kernel or system-owned files; note that most applications, including Skype, are system-owned. Accordingly, if a law enforcement penetration for the purpose of eavesdropping is executed at user level, a second exploit known as a “local privilege escalation”<sup>110</sup> attack is needed. This second attack gives the program elevated privileges and hence the ability to change device drivers, modify files, etc.<sup>111</sup> While the two exploits are generally independent, frequently both are necessary; this complicates the attack.

¶164 There is one special case worth mentioning. Some daemons run with full system privileges; if these have faulty implementations of network protocols, only a single attack is needed. This is a venerable technique, going back to the first Internet worm.<sup>112</sup> While

---

<sup>107</sup> Even a brief explanation of this is well beyond the scope of this paper. The primary problems are the nature of I/O APIs—they are generally designed to copy essential parameters from application level—and the difficulty of waiting for an I/O operation to complete without a “process context.” See, e.g., TANENBAUM & WOODHULL, *supra* note 106.

<sup>108</sup> It is generally believed that since kernels do almost no processing of network packet contents (as opposed to their “headers”), they are therefore much less vulnerable to attacks. This is more generally true, too. Having a virus-infected attachment in an email message is harmless; by contrast, clicking on it causes the attachment to be processed and thus causes damage.

<sup>109</sup> A significant percentage of software downloaded via peer-to-peer networks contains malware. See, e.g., Michal Kryczka et al., *TorrentGuard: Stopping Scam and Malware Distribution in the BitTorrent Ecosystem 1* (2012), <http://arxiv.org/pdf/1105.3671v3.pdf>; Andrew D. Berns & Eunjin (EJ) Jung, *Searching for Malware in BitTorrent 4* (2008), available at <http://www.cs.uwlax.edu/~aberns/UICS-08-05.pdf>. Note that much of this is “key generation or activation utility[ies]”; i.e., tools used to steal software. *Id.*

<sup>110</sup> For more detail on privilege escalation, including an example, see GREG HOGLUND & GARY MCGRAW, *EXPLOITING SOFTWARE: HOW TO BREAK CODE 151–53* (2004). For an additional example of a local privilege escalation attack as a proof-of-concept, see Posting of Stefan Kanthak, *Defense in Depth – the Microsoft Way (Part 11): Privilege Escalation for Dummies*, SECURITY FOCUS, <http://www.securityfocus.com/archive/1/528955/30/90/threaded>. “Local” indicates that the attacker must already have the ability to run code on the targeted system; it cannot be done by a “remote” attacker, i.e., one who can only make network connections to the machine.

<sup>111</sup> On Windows, the privileged user is known as “Administrator.” On Unix-like systems, including MacOS and Linux, it is known as “root.”

<sup>112</sup> See, e.g., EUGENE SPAFFORD, *THE INTERNET WORM PROGRAM: AN ANALYSIS 4–6* (Dec. 1988), available at <http://docs.lib.purdue.edu/cgi/viewcontent.cgi?article=1701&context=cstech>; Jon A. Rochlis & Mark W. Eichin, *With Microscope and Tweezers: The Worm from MIT's Perspective*, 32 COMM. ACM 689

modern system designs try to avoid daemons with full privileges,<sup>113</sup> in some situations this is unavoidable.

¶165 Historically, some applications have been considerably more vulnerable to user level attacks than others; these applications include web browsers and PDF viewers. As noted, modern operating systems often run these programs in sandboxes to prevent theft of or damage to user files. Sandboxes may also deny the confined program the ability to run other system commands that may be utilized for privilege escalation. Accordingly, a third exploit may be necessary to escape from the sandbox; subsequently, privilege escalation is used as before.

¶166 To summarize, there are many different points for initial attack, and all have their limitations. System privileges are needed to modify applications or device drivers and can be obtained via either a direct kernel attack, an attack on a system-level daemon, or via privilege escalation following an application level penetration.

### C. *Why Vulnerabilities Will Always Exist*

¶167 We are suggesting use of pre-existing vulnerabilities for lawful access to communications. To understand why this is plausible, it is important to know a fundamental tenet of software engineering: bugs happen. In his classic *The Mythical Man-Month*, Frederick Brooks explained why:

First, one must perform perfectly. The computer resembles the magic of legend in this respect, too. If one character, one pause, of the incantation is not strictly in proper form, the magic doesn't work. Human beings are not accustomed to being perfect, and few areas of human activity demand it. Adjusting to the requirement for perfection is, I think, the most difficult part of learning to program.<sup>114</sup>

¶168 Because computers, of course, are dumb—they do exactly what they are told to do—programming has to be absolutely precise and correct. If a computer is told to do something stupid, it does it, while a human being would notice there is a problem. A person told to walk 50 meters then turn left would realize that there was an obstacle present, and prefer the path 52 meters down rather than walking into a tree trunk. A computer would not, unless it had been specifically programmed to check for an impediment in its path. If it has not been programmed that way—if there is virtually any imperfection in code—a bug will result. The circumstances which might cause that bug to become apparent may be rare, but it would nonetheless be a bug.<sup>115</sup> If this bug should happen to be in a security-critical section of code, the result may be a vulnerability.

¶169 A National Research Council study described the situation this way:

---

(June 1989).

<sup>113</sup> The design principle is known as “least privilege.” See SHIREY, *supra* note 95.

<sup>114</sup> FREDERICK P. BROOKS JR., *THE MYTHICAL MAN-MONTH* 8 (Anniversary ed. 1995).

<sup>115</sup> In one classic incident, a single missing hyphen in a program contributed to the loss of the Mariner 1 space probe. See *Mariner 1*, NASA, <http://nssdc.gsfc.nasa.gov/nmc/spacecraftDisplay.do?id=MARIN1> (last visited Sept. 26, 2013).

[A]n overwhelming majority of security vulnerabilities are caused by “buggy” code. At least a third of the Computer Emergency Response Team (CERT) advisories since 1997, for example, concern inadequately checked input leading to character string overflows (a problem peculiar to C programming language handling of character strings). Moreover, less than 15 percent of all CERT advisories described problems that could have been fixed or avoided by proper use of cryptography.<sup>116</sup>

¶70 It would seem that bugs should be easy to eliminate: test the program and fix any problems that show up. Alas, bugs can be fiendishly hard to find, and complex programs simply have too many possible branches or execution paths to be able to test them all.<sup>117</sup>

¶71 Brooks includes a diagram on bugs comparing the predicted and actual rate of bugs in complex code.<sup>118</sup> The projection assumed a slow start, a rapid increase in the debugging rate, and a leveling off that suggested the last bugs had been found. Instead, the rate never leveled off, and the total number of bugs found was significantly higher than had been forecast.<sup>119</sup> Brooks himself suggests that testing takes about half of total development time.<sup>120</sup> However, even this is not enough: “Testing shows the presence, not the absence of bugs.”<sup>121</sup>

¶72 We will not recount the myriad techniques other than testing that have been tried in an effort to eliminate bugs; let it suffice to say there have been many. These include formal mathematical methods, better programming and debugging tools, different organizational and procedural schemes, improved programming languages, and more. Many of these ideas have helped, but none have proved a panacea. The ability to produce error-free code is the Holy Grail of systems development: heavily desired but unattainable.<sup>122</sup>

---

<sup>116</sup> TRUST IN CYBERSPACE 110 (Fred B. Schneider ed., 1999).

<sup>117</sup> The single capability that gives a computer most of its power is the ability to do things conditionally. That is, it can test a condition—is this number greater than zero? does this string of characters contain an apostrophe? is there room on the page for another line?—and continue along one program path or another, depending on the result of the test. In principle, each conditional operation can double the number of possible execution paths. (The reality is not quite that bad, because not all tests are independent.) This means that a program with just 20 conditionals may have more than  $2^{20}$ —over 1,000,000—possible paths through it; one with 40 conditionals (a very tiny number for a realistic program) may have more than 1,000,000,000,000. Exhaustive testing is not possible under these circumstances.

<sup>118</sup> See BROOKS, *supra* note 114, at 92. The diagram is a previously unpublished one by John Harr.

<sup>119</sup> Neither the graph nor the text make it clear whether the graph ended because the project was finished or simply because it was a snapshot of a single year’s experience and did not look at the entire project. The graph, presented at the 1969 Spring Joint Computer Conference, shows one year of experience building the #1 ESS; the programming undoubtedly took longer. See PHIL LAPSLEY, *EXPLODING THE PHONE* 233–38 (2013). The switch itself is described in Keister, Ketchledge & Vaughan, *supra* note 87. New versions of the code were unlikely to have fewer bugs; rather, the bug rate *increases* after some point. BROOKS, *supra* note 114, at 53–54.

<sup>120</sup> See BROOKS, *supra* note 114, at 10, 17 (explaining the complexity of the model).

<sup>121</sup> SOFTWARE ENGINEERING TECHNIQUES: REPORT ON A CONFERENCE SPONSORED BY THE NATO SCIENCE COMMITTEE, ROME, ITALY, 27TH TO 31ST OCTOBER 1969 16 (1970) (quoting E. W. Dijkstra).

<sup>122</sup> Operational errors are common, too. See, e.g., Barton Gellman, *NSA Broke Privacy Rules Thousands of Times Per Year, Audit Finds*, WASH. POST, Aug. 16, 2013, [http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125\\_story\\_1.html](http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story_1.html) (“One in 10 incidents is attributed to a typographical error in which an analyst enters an incorrect query and retrieves data about U.S. phone calls or e-mails.”). Another bug confused the country and city codes for Cairo, Egypt (20 2) with the area code for Washington, D.C. (202). *Id.* These sorts of errors led to literally thousands of

¶73 When we are dealing with computer security, though, the question is somewhat different than whether the program has bugs. Rather, the proper question is whether the security-sensitive parts of the system have bugs. When formulated this way, there would seem to be an obvious solution: divide a complex system up into security-sensitive and security-insensitive pieces; bugs in the latter, though annoying, would not result in disaster. Such an approach would also improve the correctness of the security-critical components. The bug rate in code increases more than linearly with the size of the program; therefore, a program that is twice as large has more than twice as many bugs. Perhaps the security-sensitive section, which is by definition smaller, would thereby have far fewer bugs than the system as a whole.

¶74 This approach has been at the heart of most secure system designs for more than fifty years. It was set out mostly clearly in the so-called “Orange Book,” the 1985 Department of Defense criteria for secure operating system design.<sup>123</sup> The Orange Book prescribed something called a “Trusted Computing Base,” the security-essential portions of a system:

The heart of a trusted computer system is the Trusted Computing Base (TCB) which contains all of the elements of the system responsible for supporting the security policy and supporting the isolation of objects (code and data) on which the protection is based. The bounds of the TCB equate to the “security perimeter” referenced in some computer security literature. In the interest of understandable and maintainable protection, a TCB should be as simple as possible consistent with the functions it has to perform.<sup>124</sup>

¶75 This dream has proved elusive for two very different reasons. First, modern TCBs are themselves extremely large, significantly bigger than the entirety of the 1970s and 1980s vintage systems. Although modern software is far more reliable, that does not translate into absolute reliability. It is worth noting that one of today’s complex applications is tens of times larger than entire systems from the 1980s, when the Orange Book was written; this complexity, as we have noted, leaves them very vulnerable to attack. Today’s operating systems are also vastly larger. Second, the notion of the TCB is less clear than it once was. More and more serious security incidents target components that fit no one’s definition of “trusted,” but the attacks are effective nevertheless. For example, in 1988 the very first Internet worm exploited holes outside what would likely have been considered part of the TCB.<sup>125</sup> In essence, although not by intent, it was a

---

incidents of improper collection of surveillance data.

<sup>123</sup> DEP’T OF DEF., DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA (1985) available at <http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt>. The nickname comes from the color of its cover; it is part of a series of publications known collectively as “The Rainbow Series.”

<sup>124</sup> *Id.* at 65.

<sup>125</sup> The worm tried by various means to find and attack other computers. If it ever succeeded, it sent a copy of itself over to those computers and started executing there as well; meanwhile, the first copy continued to scan for other targets. There was no check to make sure that a given computer was infected only once; this meant that vulnerable systems were running very many copies of the worm, sufficiently many that legitimate programs were crowded out. Furthermore, the Internet itself was clogged by the attack traffic. Finally, since one of the vulnerable services was email, many sites turned off their mail systems in an attempt to protect themselves; this, however, hindered coordination of attempts to combat the worm since many people knew no other way to reach their colleagues at other sites. See SPAFFORD, *supra* note



denial of service attack: it consumed most of the capacity of the infected machines. This happened at the user level; the affected programs were not part of the TCB.<sup>126</sup> Put another way, trying to break up the system into trusted and untrusted parts does not work as well as had been hoped; bugs anywhere can be and have been exploited by malware.

¶176 We conclude that for the foreseeable future, computer systems will continue to have exploitable, useful holes. The distinction between flaws in the TCB and flaws outside of it is important. Non-TCB programs—frequently known as “user mode” or “application mode” programs—have the privileges of the user who runs them, whereas TCB programs are generally all-powerful and have access to more files and the ability to change them.<sup>127</sup>

#### D. *Why the Vulnerability Solution Must Exist Anyway*

¶177 Considering lawful intercept purely as an economic question, it is tempting to ask which is a cheaper solution: a vulnerability-based approach or a CALEA-like law. The question, however, is not that simple. Even apart from our overriding theme—that applying CALEA to Internet software creates many very serious risks to both security and innovation—and apart from the cost-shifting issue (with CALEA-like solutions, the bulk of the cost is not carried by law enforcement), there is a further, more fundamental issue: a vulnerability-based intercept capability must exist regardless of any extension of CALEA. The question, then, is not which costs less, but whether the incremental cost of CALEA is justifiable given that the vulnerability-based approach must be pursued in any case.

¶178 No matter what a CALEA-like law says, there will always be important situations where CALEA interfaces will not help law enforcement conduct surveillance. Often, these will be extremely important, urgent situations involving national security, counterterrorism, or major drug gangs.<sup>128</sup> Those criminals involved in national security and counterterrorism are more likely than common criminals to use non-American or even custom-written communications software and procedures.<sup>129</sup> Other situations in which a new law will not help include situations with people who use older software that has not been upgraded to include a lawful intercept feature, and more generally situations

---

112, and Rochlis & Eichen, *supra* note 112, for more details on the worm’s behavior and structure.

<sup>126</sup> This is not strictly true. For technical reasons, one of the programs that were successfully attacked did run with elevated privileges; however, neither the penetration nor the excess resource consumption by it were related to those privileges. It ran as privileged (and hence by definition as part of the TCB) because the importance of avoiding excess privilege was not as well understood in the general community at that time as it is today.

<sup>127</sup> This stark dichotomy between all-powerful and relatively powerless code is generally seen by the computer security and operating system communities as a bad idea. Many schemes have been proposed to create intermediate levels of privilege; few, if any, have caught on *and* been more than minimally effective at protecting the system. There has been more success of late with sandboxes.

<sup>128</sup> The Mexican Zeta drug gang uses a home-built, encrypted radio network. See Michael Weissenstein, *Mexico’s Cartels Build Own National Radio System*, YAHOO! NEWS (Dec. 27, 2011), <http://news.yahoo.com/mexicos-cartels-build-own-national-radio-system-200251816.html>.

<sup>129</sup> The Russian sleeper agent ring arrested in 2010 used special programs for *steganography*, a way of concealing the very existence of messages. See Noah Shachtman, *FBI: Spies Hid Secret Messages on Public Websites*, WIRED (June 29, 2010, 1:11 PM), <http://www.wired.com/dangerroom/2010/06/alleged-spies-hid-secret-messages-on-public-websites/>.

with any communications application that automatically provides end-to-end encryption capability.<sup>130</sup>

¶79 In situations like these, where the case is important and built-in lawful intercept mechanisms are not available, using vulnerabilities becomes an attractive alternative. The alternative to using vulnerabilities—a so-called “black bag job” or a covert search—is far riskier.<sup>131</sup> Electronically placing a vulnerability on a machine does not put a law-enforcement agent at risk; conducting a black-bag job or a covert search certainly does.

¶80 As with so much other high technology, using vulnerabilities for eavesdropping has a relatively high start-up cost, whereas continued use does not. Apart from the obvious drop in the cost per interception, the operational software is likely to improve over time. That is, as the developers have more time and gain more experience, the overall package will improve. It will provide more functionality, higher efficiency, and stronger resistance to detection. The actual exploits used will, as noted, change over time; however, the exploits are likely to be usable in many more interceptions than in a CALEA-based world, which will also drive down the cost of each interception. In other words, and to a much greater degree than in a CALEA-based approach, using vulnerabilities will improve law enforcement’s abilities in all cases, especially the most critical ones.

#### IV. VULNERABILITY MECHANICS

¶81 In this section, we examine the potential use of vulnerabilities. We begin by exploring warrant issues for using exploits to wiretap. We discuss how vulnerabilities may be exploited, and consider minimization in this environment and what tools and procedures are available that law enforcement authorities might use or modify to gain access. We also discuss the vulnerability and exploit markets. Finally, we discuss what steps would be needed for productizing an exploit specifically for lawful access by law enforcement.

##### A. Warrant Issues

¶82 Obviously, any use of vulnerabilities for wiretapping requires proper authorization. However, because of the technologies involved, the process for obtaining proper authorization may be somewhat more involved than for conventional wiretaps.

¶83 One issue is that there are two distinct steps: exploiting the vulnerability, i.e., hacking the target’s machine with proper permission, and actually carrying out the desired interception. Arguably, two different court orders should be obtained. Documents released under the Freedom of Information Act show the FBI has used such a two-step process to obtain information in at least one situation. The FBI first sought a search warrant to install Computer and Internal Protocol Address Verifier (CIPAV) on the

---

<sup>130</sup> Even the current CALEA statute states: “A telecommunications carrier shall not be responsible for decrypting, or ensuring the government’s ability to decrypt, any communication encrypted by a subscriber or customer, unless the encryption was provided by the carrier and the carrier possesses the information necessary to decrypt the communication.” 47 U.S.C. § 1002(b)(3) (2006). The “information necessary to decrypt the communications” is typically a cryptographic key. If end-users do their own key management, the provider is unlikely to have the keys.

<sup>131</sup> Such searches are performed when necessary. *See, e.g.*, Schactman, *supra* note 129.

target's machine, which sends address and protocol information from the target's machine to the FBI.<sup>132</sup> Having obtained the IP address and other relevant information by conducting surveillance, the FBI then sought a pen register/trap-and-trace order from the court; however, this is not always done. In *In Re Warrant to Search a Target Computer at Premises Unknown*, the FBI submitted a single Rule 41 warrant application, covering all activities: finding the target, installing their own software, gathering addresses, taking pictures, etc.<sup>133</sup>

¶84 Another issue that can cause complications is the need for "technical reconnaissance" to identify the proper target machine.<sup>134</sup> This may involve listening to other conversations, which would presumably require its own authorization.

¶85 Finally, the design of this sort of tap presents some opportunities for minimization by technical means, prior to the usual minimization that is required by law.<sup>135</sup> Arguably, this should be specified in the warrant as well.<sup>136</sup>

### B. Architecture

¶86 How should a law enforcement exploit software platform be designed? The special legal requirements, the technical quirks involved in exploitation, the speed with which technology changes, the lifetime of a vulnerability, the need for non-proliferation, and even budgetary constraints all suggest that any framework of tools developed for surveillance must be easily configurable and readily adaptable. This in turn suggests that a highly modular architecture is needed for a vulnerability-based communications intercept vehicle.<sup>137</sup>

---

<sup>132</sup> See Jennifer Lynch, *New FBI Documents Provide Details on Government's Surveillance Spyware*, ELECTRONIC FRONTIER FOUND. (Apr. 29, 2011), <https://www.eff.org/deeplinks/2011/04/new-fbi-documents-show-depth-government>. CIPAV is a current FBI software package analogous to what we are proposing here. Its capabilities, as described in an affidavit for a search warrant, include collecting the target machine's IP address, MAC address, operating system type and version, browser type and version, "certain registry-type information," last URL visited, etc. See Affidavit for State of Washington, County of King, In the Matter of the Search of any Computer Accessing Electronic Message(s) Directed to the Administrator(s) of MySpace Account "Timberlinebombinfo" and Opening Message(s) Delivered to that Account by the Government (No. MJ07-5114), at 3, *available at* <http://politechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf>.

<sup>133</sup> No. H-13-234M, 2013 WL 1729765 (S.D. Tex. Apr. 22, 2013). Mark Eckenwiler, formerly a top Justice Department authority on surveillance, has indicated that intrusions needed to execute pen register orders can be performed solely on the lesser pen register standard. See Jennifer Valentino-DeVries & Danny Yadron, *FBI Taps Hacker Tactics to Spy on Suspects*, WALL ST. J., Aug. 3, 2013, <http://online.wsj.com/article/SB10001424127887323997004578641993388259674.html>.

<sup>134</sup> See *infra* Section IV.D.

<sup>135</sup> Minimization is as defined in the wiretap statute, 18 U.S.C. § 2518(5) (2006) ("Every order and extension thereof shall contain a provision that the authorization to intercept . . . shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective . . .").

<sup>136</sup> See *infra* Section IV.C.

<sup>137</sup> Designing systems to use modules is standard software engineering practice. By definition, modules communicate via well-defined interfaces, allowing easy substitution of different versions. See, e.g., D.L. Parnas, *On the Criteria to be used in Decomposing Systems into Modules*, 15 COMM. ACM 1053, 1053-54 (1972). A good example of a modular framework is a picture editor. Many different file formats—JPEG, TIFF, PNG, etc.—can be imported into a picture editor. The editing is done in the same way, regardless of the input format; then, the new version can be stored in any of these formats. In other words, the file format input/output routine is a separate module. The same is true for vulnerability-based surveillance. With a well-designed framework, execution of a wiretap could be as simple as choosing a wiretap module, an

¶87 The particular components to be used against any given target will vary widely. Consider the choice of initial exploit. For a target with an older (and unpatched) system, an older and publicly-known exploit might be sufficient, but for wiretapping someone using a newer operating system, or one that is fully patched, an old vulnerability will not suffice, forcing the use of a newer one. Further, another target, not using the common application targeted by either of the previous two, might require yet a third vulnerability. Any of these exploited weaknesses could potentially be closed on the targets' systems at any time, which could require the use of yet another vulnerability.<sup>138</sup>

¶88 There are other considerations as well. If only voice communications are to be picked up, there is no need to include a module providing keystroke-logging capability in the payload. Indeed, the less code that is included, the less the risk of the tap being discovered. Perhaps more important, code that is not included cannot be repurposed by someone else, thus aiding in non-proliferation.<sup>139</sup> Beyond that, selective inclusion aids in warrant compliance, by limiting what is collected to what the court's order permits. This is discussed in more detail below.<sup>140</sup>

¶89 A modular framework can also be extremely cost-effective relative to other designs. By design modules are plug-and-play—no matter how different they may be on the inside, the way the modules communicate with the framework is standardized. The design makes it easy to have many different people develop exploits for the same framework, and straightforward for people to use new ones. When an exploit becomes obsolete, only the module containing that exploit needs to be rewritten or replaced. Pre-configured warrant modules provide assurance to law enforcement that exploits will collect the communications they need,<sup>141</sup> and assurance to the judge that the exploit and payload will behave as specified in the warrant. If the investigation changes and a new warrant module is needed, the exploit executable only needs to be recompiled with the new module and reinstalled.

### C. *Technical Aspects of Minimization*

¶90 The wiretap statute specifies that: “Every order and extension thereof . . . shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter . . . .”<sup>142</sup> While this is normally a matter for judges to rule on, a properly designed intercept package can carry out some of this task. This provides greater privacy for individuals not targeted by the warrant. More subtly, by automatically eliminating a lot of the extraneous content, it eases the task of humans charged with minimization and thus likely reduces their error rate.<sup>143</sup>

---

exploit, and warrant information, entering the target information, and pressing “Go.” The system would then build the payload for automatic installation. New exploits or new warrant information would be separate modules; the rest of the program would not be affected.

<sup>138</sup> See discussion of the lifetime of these components, *infra* Section IV.E.

<sup>139</sup> See *infra* Section V.

<sup>140</sup> See *infra* Section IV.C.

<sup>141</sup> See *id.*

<sup>142</sup> 18 U.S.C. § 2518(5) (2006).

<sup>143</sup> While we do not suggest or think that a program can perform full minimization, it can certainly carry out mechanical aspects, e.g., excluding services and perhaps users not covered by the warrant.

¶91 A warrant must clearly specify what communications may and may not be collected:

Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify—

(a) the identity of the person, if known, whose communications are to be intercepted; . . .

(c) a particular description of the type of communication sought to be intercepted<sup>144</sup>

¶92 Intercepts that collect more than is authorized are legally problematic, to say the least.<sup>145</sup>

¶93 A modular architecture greatly simplifies the execution of the warrant. Modules for common warrant specifications would contain pre-configured values, such as types of data to collect or ignore, specified ports to listen on, and time limits. The framework would compile these values into a properly tailored exploit executable automatically, without the need for any special configuration by the law enforcement technicians.<sup>146</sup>

---

<sup>144</sup> 18 U.S.C. § 2518(4).

<sup>145</sup> According to documents obtained by the Electronic Privacy Information Center under FOIA, when the FBI's UBL unit (Usama bin Laden unit) was conducting FISA surveillance, "The software was turned on and did not work correctly. The FBI software not only picked up the E-Mails under the electronic surveillance of the FBI's target, [redacted] but also picked up E-Mails on non-covered targets. The FBI technical person was apparently so upset that he destroyed all the E-Mail take, including the take on [redacted] is under the impression that no one from the FBI [redacted] was present to supervise the FBI technical person at the time." Memorandum from [redacted] to Spike (Marion) Bowman (Apr. 5, 2000), available at <http://www.epic.org/privacy/carnivore/fisa.html>.

<sup>146</sup> "Compilation" is the process of turning human-readable "source code," written in a language like C or C++, into the string of bytes that are actually understood by the underlying hardware. At compilation time, it is possible to select which sections of the program should be included in the eventual module. A classic treatment of how compilers work can be found in ALFRED V. AHO, MONICA S. LAM, RAVI SETHI & JEFFERY D. ULLMAN, COMPILERS: PRINCIPLES, TECHNIQUES, AND TOOLS (2nd ed. 2007).

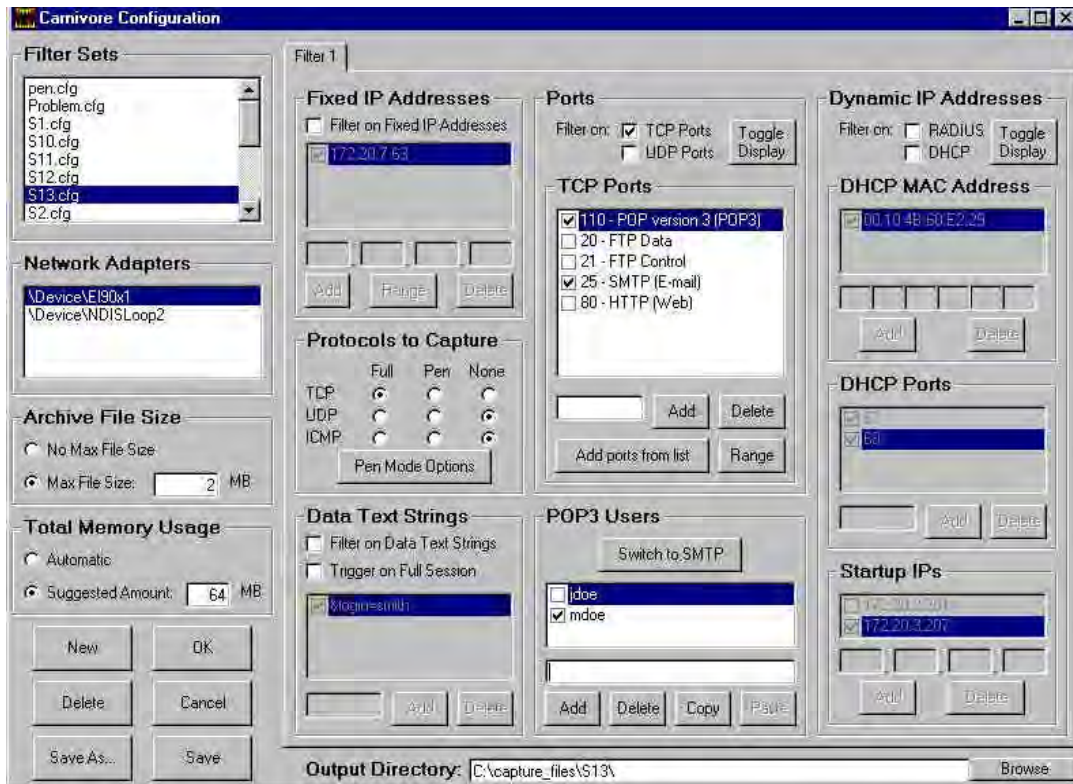


Figure 2: A sample warrant configuration screen from Carnivore. This filter is set up to intercept all inbound (POP) and outbound (SMTP) email from user mode.

¶94 The warrant configuration screen<sup>147</sup> from the (now obsolete) Carnivore wiretapping system<sup>148</sup> provides a useful example. It has options for full content and pen register capture, fields for identifying which protocols should be captured, which IP addresses or users should have their data monitored, and so on. A similar scheme should be used here, with a crucial difference: modules not selected would not be included in the payload installed on the target's machine.

¶95 Other information can also be used for minimization. Assume, for example, that police know from other means that their suspect uses only one of the user profiles (i.e., logins) on a shared computer.<sup>149</sup> The intercept module, if properly configured, would operate only when that user is logged in. Similar filters could be used for communications applications like Skype that have their own logins.

<sup>147</sup> This image is taken from Figure C-16 of STEPHEN P. SMITH, HENRY H. PERRITT, JR., HAROLD KRENT, STEPHEN MENCIK, J. ALLEN CRIDER, MENG FEN SHYONG & LARRY L. REYNOLDS, IIT RES. INST., INDEPENDENT REVIEW OF THE CARNIVORE SYSTEM: FINAL REPORT C-17 (2000) (aspect ratio adjusted), available at [http://www.epic.org/privacy/carnivore/carniv\\_final.pdf](http://www.epic.org/privacy/carnivore/carniv_final.pdf).

<sup>148</sup> Carnivore was later renamed as the DCS 1000, and has since been retired in favor of commercial solutions. The apparent abandonment of the package is discussed in the 2002 and 2003 FBI reports to Congress. FED. BUREAU OF INVESTIGATION & U.S. DEP'T. OF JUST., CARNIVORE/DCS-1000 REPORT TO CONGRESS 3 (Feb. 24, 2003), available at [https://epic.org/privacy/carnivore/2002\\_report.pdf](https://epic.org/privacy/carnivore/2002_report.pdf); FED. BUREAU OF INVESTIGATION & U.S. DEP'T. OF JUST., CARNIVORE/DCS-1000 REPORT TO CONGRESS 4 (Dec. 18, 2003), available at [https://epic.org/privacy/carnivore/2003\\_report.pdf](https://epic.org/privacy/carnivore/2003_report.pdf).

<sup>149</sup> This is sometimes the case. See, e.g., *State of Ohio v. Nicholas J. Castagnola*, Nos. CR 10 07 1951 (B) & CR 10 08 2244, slip op. at 11–14 (Mar. 29, 2013).

#### D. Technical Reconnaissance

¶96 The reconnaissance phase—learning enough about the target to install the necessary monitoring software—is essential to a successful compromise of a device. Because exploits must be exquisitely tailored to particular versions and patch levels, using the wrong exploit frequently results in failures, and can even raise alerts or cause suspicious crashes. There are a number of widely used, readily available tools. Many of the best tools are even available in a free, ready-to-use downloadable toolbox; for example, the Backtrack-Linux Penetration Testing Distribution.<sup>150</sup>

¶97 The most common first step is to check publicly available information. DNS<sup>151</sup> and Whois<sup>152</sup> lookups are used to find Internet domain and IP information. Simple use of search engines and scouring social media sites often provide some information about the target’s operating system, cell phone platform, service provider, and commonly used applications. With the appropriate legal process, e.g., a subpoena or court order under 18 U.S.C. § 2703(d) (2006), some of this information may also be available from the service provider.

¶98 If the investigators have access to some emails from the target, a great deal of information may be found by studying the headers. An examination of some of our test emails showed such lines as:

Mime-Version: 1.0 (Mac OS X Mail 6.2 \ (1499\))  
X-Mailer: Apple Mail (2.1499)

and

X-Mailer: iPhone Mail (10B146).

which are rather clear indicators of which operating system is in use.

¶99 To remotely access a machine, an attacker generally needs to know the IP and/or MAC addresses of the machine,<sup>153</sup> the operating system (including exact version and

---

<sup>150</sup> The Backtrack Linux Penetration Testing Distribution is an open-source, ready-to-use linux operating system specifically customized and configured for security analysts and penetration testers. It can be installed onto a computer or booted live from a disk or thumbdrive. It contains a comprehensive set of tools for network and system scanning, vulnerability detection, exploitation, privilege escalation and forensics. There are also tutorials and How-To’s available and a large user and contributor community. *See BackTrack Linux*, BACK|TRACK-LINUX.ORG, <http://www.backtrack-linux.org> (last visited Nov. 12, 2013).

<sup>151</sup> The DNS—the Domain Name System—is used to convert human-friendly names such as [www.fbi.gov](http://www.fbi.gov) to the number IP address understood by low-level Internet hardware. Information in the DNS is especially useful when trying to break into organizations rather than individual users’ computers. *See, e.g.,* WILLIAM CHESWICK, STEVEN M. BELLOVIN & AVIEL D. RUBIN, FIREWALLS AND INTERNET SECURITY 31–33 (2d ed. 2003).

<sup>152</sup> Whois is a public database lookup service provided by the Internet name registrars that provides information about the ownership of domain names, address blocks, etc. For more information, see Simone Carletti, *Understanding the WHOIS Protocol*, SIMONE CARLETTI’S BLOG (Mar. 27, 2012, 12:13 PM), <http://www.simonecarletti.com/blog/2012/03/whois-protocol/>, which gives examples of Whois output.

<sup>153</sup> IP and MAC addresses are networking concepts. MAC addresses are generally hard-wired in a computer’s communications hardware, though sophisticated users can change them. IP addresses are often transient, but tend to remain the same for a given computer in a given location. While IP addresses are typically assigned by the network administrator of the site at which the computer is located, MAC addresses are assigned by the manufacturer and therefore indicate the computer type and model. *See, e.g.,* ANDREW TANENBAUM, COMPUTER NETWORKS (4th ed. 2003).

patch level), what services are running on the machine, which communications ports are open,<sup>154</sup> what applications are installed, and whether the system contains any known vulnerabilities. This process of discovery is referred to as “Mapping” and “Enumeration.”<sup>155</sup>

¶100 Mapping can be of the system or of the network (or both). Network mapping can be WiFi or Ethernet, and can refer to finding hidden networks, or to enumerating all the devices and their addresses connected to a particular network. Mapping the target device or system requires finding the so-called “MAC address,” a hardware address transmitted when speaking over Ethernet, WiFi, or Bluetooth networks. If the target of a tap is using a smartphone at a public hotspot, detecting that person’s MAC address could, for example, reveal what brand of phone is being used.

¶101 Another way to ascertain the system version is to perform “OS fingerprinting.” OS fingerprinting involves looking for subtle differences in the network protocol implementations of different operating systems, and in particular the response of the system being examined to various probes. NMAP, a freely available popular network security tool, is most commonly used. In addition to OS fingerprinting, NMAP provides open service and open port identification and limited vulnerability scanning.<sup>156</sup>

¶102 The final step in the information-gathering phase is to scan the target system to see if it has common vulnerabilities.<sup>157</sup>

### *E. Finding Vulnerabilities*

¶103 Once the target has been adequately identified and scanned, a suitable vulnerability must be identified. The primary criterion, of course, is compatibility with the user’s operating system; another crucial criterion is mode of delivery. Some exploits, for example, can be delivered by email messages; others require the user visiting a particular web page, or opening a file containing a specific, vulnerable application. Email delivery is easiest because it does not require the user to take any particular action, but apart from

<sup>154</sup> On networked computer systems, services offered are assigned to particular (and generally standardized) “port numbers,” a more or less arbitrary value between 1 and 65535. Port enumeration is the process of seeing what ports, and hence what services, are available on a given system. Using open ports for intrasystem communication, rather than more secure alternatives, was one of the items cited in the FTC complaint against HTC. *See* Complaint at 3–4, *In re* HTC America, Inc., No. C-4406 (F.T.C. June 25, 2013).

<sup>155</sup> “Mapping” is standard networking terminology for discovery of the computers on a network and the topology of the network itself; the word is even part of the name “NMAP.” *See infra* note 156. “Enumeration” is defined in *Network Enumerators*, SECURITY WIZARDRY, <http://www.securitywizardry.com/index.php/products/scanning-products/network-enumerators.html> (last visited Jan. 6, 2014), though to some extent it is just a technical computer science term for learning a set of things, as opposed to “brute force” which is trying all possibilities to find one secret.

<sup>156</sup> GORDON “FYODOR” LYON, *NMAP NETWORK SCANNING: OFFICIAL NMAP PROJECT GUIDE TO NETWORK DISCOVERY AND SECURITY SCANNING* xxi–xxii, 205 (2008).

<sup>157</sup> There are a number of widely-used vulnerability scanning systems. Nessus (available from <http://www.tenable.com/products/nessus>) is the most widely used one; it can scan for thousands of vulnerabilities and plug-ins, and even provides detailed mobile device information like serial numbers, model, version, and last connection timestamps. *See* TENABLE NETWORK SEC., *NESSUS: THE WORLD’S MOST TRUSTED VULNERABILITY SCANNER* (2013), available at <https://static.tenable.com/datasheets/nessus-datasheet.pdf>. Another popular vulnerability scanning system is Nexpose (available from <https://www.rapid7.com/products/nexpose/>).



the fact that it might be noticed there is always the risk that a spam filter will catch it.<sup>158</sup> Another class of exploits requires being on the same local network<sup>159</sup> as the victim, or on an interconnected network if there are no intervening firewalls.<sup>160</sup> Even infected USB flash drives have been used; indeed, the Stuxnet attack on the Iranian nuclear centrifuge plant is believed to have started that way.<sup>161</sup>

¶104 Many exploits are publicly announced,<sup>162</sup> and are often available in easy-to-launch pre-packaged scripts. The Metasploit Project hosts the largest database of these scripted, publicly available exploits (called “modules”).<sup>163</sup> These modules can be utilized by a number of different exploitation applications, such as the Metasploit Framework and Core Impact Pro.<sup>164</sup> The National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) lists all known vulnerabilities, including what versions of what systems are affected and references to more information (but no exploit information). Information about the exploit, including an executable script or some proof-of-concept source code, is often published on one of a number of well-regarded websites and public mailing lists.<sup>165</sup>

---

<sup>158</sup> Sending email messages crafted to appear genuine to a particular target is known as “spear-phishing.” In skilled hands, spear-phishing is extremely effective. Press reports suggest that is one of the primary schemes used by cyberespionage units. *See, e.g.*, Jaikumar Vijayan, *DHS Warns of Spear-phishing Campaign Against Energy Companies*, COMPUTERWORLD (Apr. 5, 2013, 4:03 PM), [https://www.computerworld.com/s/article/9238190/DHS\\_warns\\_of\\_spear\\_phishing\\_campaign\\_against\\_ene\\_rgy\\_companies](https://www.computerworld.com/s/article/9238190/DHS_warns_of_spear_phishing_campaign_against_ene_rgy_companies).

<sup>159</sup> A LAN (Local Area Network) is generally a high-speed network that covers a relatively small area. Typical LANs include most home networks, WiFi hotspots, or, in an enterprise, a single department. LANs are interconnected to each other or to WANs (Wide Area Network) by *routers*. *See, e.g.*, ANDREW TANENBAUM & DAVID WETHERALL, *COMPUTER NETWORKS* (5th ed. 2010).

<sup>160</sup> Most home routers are technically known as Network Address Translators (NATs). For these purposes, NATs serve the same purpose as firewalls; these attacks cannot be launched at a target that is behind a NAT. *See* Geoff Houston, *Anatomy: A Look Inside Network Address Translators*, INTERNET PROTOCOL J., Sept. 2004, *available at* [http://www.cisco.com/web/about/ac123/ac147/archived\\_issues/ipj\\_7-3/ipj\\_7-3.pdf](http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-3/ipj_7-3.pdf).

<sup>161</sup> *See Stuxnet Dossier, supra* note 17, at 3. It is unclear how the infected flash drive was introduced. *See, e.g.*, James Bamford, *The Secret War*, WIRED (June 12, 2013, 9:00 PM), <http://www.wired.com/threatlevel/2013/06/general-keith-alexander-cyberwar/all/>.

<sup>162</sup> The US Computer Emergency Readiness Team (US-CERT) maintains a frequently updated list of vulnerabilities. Security researchers and privately owned research laboratories such as Vulnerability Lab and Immunity, Inc. announce vulnerabilities on websites and Twitter when they are discovered. Verified vulnerabilities are collected, categorized, and enumerated in the comprehensible, searchable NIST NVD database. *See National Vulnerability Database*, DEP’T OF HOMELAND SEC., <http://web.nvd.nist.gov/view/vuln/search> (last visited Feb. 5, 2014)

<sup>163</sup> Each of the exploits in the database consists of a specific vulnerability packaged into a module, which can be loaded into an attack application, such as the Metasploit Framework, to run. Because of the popularity of the Metasploit Framework, many exploits sold are available as Metasploit modules. *See, e.g.*, *Metasploit Exploit*, EXPLOIT HUB, <https://exploithub.com/product-type/metasploit-exploit.html> (last visited Sept. 24, 2013).

<sup>164</sup> The Metasploit Framework, available from <http://www.metasploit.com>, is the most widely used exploitation application available today. It is available in both free and commercial versions and has a wide developer base. *See* METASPLOIT, <http://www.metasploit.com> (last visited Sept. 24, 2013). Core Impact Pro can be purchased from <http://www.coresecurity.com>.

<sup>165</sup> There are many such mailing lists. Perhaps the best-known one is BugTraq, <http://www.securityfocus.com/archive/1>.

¶105 Another group of exploits is privately held exploits; these include the zero-days described above,<sup>166</sup> as well as exploits for sale by professional security vulnerability researchers. We discuss these in detail in Section G.

¶106 Sometimes, no publicly available vulnerabilities will be usable, and the option of purchasing one from the vulnerabilities market will be undesirable or unavailable. In that case, law enforcement agents—more likely, a central “Vulnerability Lab”—must find one.<sup>167</sup> While this issue is out of scope here, we note there are many commonly available tools regularly used for finding vulnerabilities by software vendors trying to protect their products and by attackers.

¶107 Finally, in the rare case where directly compromising a target platform through an exploit is not possible, a technique known as a “Man-in-the-Middle” (MitM) attack might be used.<sup>168</sup> Such attacks involve interrupting the communications path between the target and some site the target is trying to access; the attack tool then intercepts communications intended for that resource. A successful MitM attack might be another way to launch an attack; alternatively, it could permit acquisition of passwords and account information that would provide law enforcement with access to other useful resources.<sup>169</sup>

#### F. Exploits and Productizing

¶108 While off-the-shelf exploits may be available to law enforcement on the black market, law enforcement does not require their functionality, which is installing general purpose remote-access malware to send spam, steal bank account numbers, etc. Rather, they wish to gather specific items of data authorized by the warrant, and to do so in a form suitable for presentation in court. In addition, access to a target system by a law enforcement agent must take care to preserve evidence and chain of custody.<sup>170</sup> This implies due attention to precise logging of exactly what was done, when, and by whom. Consequently, off-the-shelf exploits (as opposed to vulnerabilities) are by themselves not likely to be particularly useful to law enforcement, except as a starting point or perhaps under exigent circumstances.<sup>171</sup> What law enforcement needs are specialized

---

<sup>166</sup> See *supra* Section II.A.

<sup>167</sup> The FBI already operates the Domestic Communications Assistance Center, which apparently does at least some of this. See, e.g., *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies*, *supra* note 2, at 7 (2011) (statement of Valerie Caproni, General Counsel, Federal Bureau of Investigation); Declan McCullagh, *FBI Quietly Forms Secretive Net-Surveillance*, CNET (May 22, 2012, 11:44 PM), [http://news.cnet.com/8301-1009\\_3-57439734-83/fbi-quietly-forms-secretive-net-surveillance-unit](http://news.cnet.com/8301-1009_3-57439734-83/fbi-quietly-forms-secretive-net-surveillance-unit).

<sup>168</sup> MitM attacks can be used at any time. However, they are almost always harder to do, since they require interfering with the traffic of exactly one user who may be at an unknown location. They are also more detectable than other attacks, although only by very sophisticated users.

<sup>169</sup> Depending on the provisions of the original warrant, it may be necessary to seek a modification. In particular, a warrant permitting interception of communications does not grant the right to search stored email archives; that would require an order under the Stored Communications Act, 18 U.S.C. §§ 2701–2712 (2006).

<sup>170</sup> See Timothy M. O’Shea & James Darnell, *Admissibility of Forensic Cell Phone Evidence*, U.S. ATT’YS’ BULL., Nov. 2011, at 47–49, available at [http://www.justice.gov/usao/eousa/foia\\_reading\\_room/usab5906.pdf](http://www.justice.gov/usao/eousa/foia_reading_room/usab5906.pdf); see also U.S. DEP’T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL PROCEDURES AND CASE LAW FORMS 27–31 (June 2005), available at <http://www.justice.gov/criminal/foia/docs/elec-sur-manual.pdf> (discussing sealing intercepts to protect their integrity).

<sup>171</sup> See *infra* Section IV.G.

eavesdropping products, products that use exploits to produce legally acceptable communications intercepts, and do so as simply and as cheaply as possible while still complying with all legal requirements.

¶109 The three functional components of a law enforcement eavesdropping product—the exploit (which provides access to the system), the eavesdropping code, and the supporting infrastructure—all have different characteristics and lifetimes. Exploits have the shortest lifetime due to their specificity, installation characteristics, vendor patches, etc. Accordingly, a good methodology for use of exploits is the dropper/payload model, where the eavesdropping product is composed of two principal parts: a dropper and a specially encrypted payload *that is specifically encrypted for the particular target*. (This payload includes the second and third components.) A *penetrator* is used as the dropper, which is the initially injected code that exploits the actual vulnerability and thus gains access to the target system. Once access is acquired, the penetrator decrypts the payload. The payload is encrypted as a security measure to ensure the penetration code cannot easily be detected or reused by criminals; it also ensures that the payload targets the correct system. A payload is specifically encrypted for a particular target by using target-specific information like serial numbers, the MAC address, IP address, etc., as the key to encrypt and decrypt the payload.<sup>172</sup> The penetrator picks this information up, which would have been acquired during earlier technical reconnaissance, at payload installation time. This method protects untargeted machines from compromise: if the code is executed on the wrong machine, decryption will fail.

¶110 The payload itself should be designed to provide the access specified in the warrant with minimal changes to the target system. Those changes that are necessary should be logged and time-stamped as to provide documentation that vital evidence was neither altered nor destroyed. If the warrant includes provisions for recording communications, the payload should also contain provisions for minimization, including the ability to turn recording on and off and the length and time of communications recorded. Payloads do not change very much over time; while they may need to adapt to different major versions of operating systems, they generally rely on features not likely to change very often. Further, payloads that have already been installed are rarely disabled by vendor patches.

¶111 The supporting infrastructure (which is also part of the payload) has an intermediate lifetime. Some of the infrastructure, such as the code to set up encrypted channels to the investigators, is straightforward and not particularly tied to unusual law enforcement needs; this code will be quite long lived. The command-and-control subsystem—the mechanism with which investigators control the tap, turn recording on and off, etc.—is similarly straightforward, although the fine details will be specific to the application. Much of this code will be virtually the same even across different operating systems. On the other hand, the concealment mechanisms—the code that hides the existence of the payload from the computer’s owner and specialists who may be hired to “sweep” the computer for bugs—is likely to be highly dependent on the operating system, including the particular version, and will change fairly frequently.

---

<sup>172</sup> Encryption is accomplished through the use of an algorithm, which may be public, and a key, which is a piece of secret data. If the encryption algorithm is strong, it should be effectively impossible to decrypt the file without knowledge of the key.

¶112 It is a good idea for the payload to have a self-destruct option, perhaps the time limit set by the warrant, after which the law enforcement software restores the target system to its pre-exploit state, erases itself, and removes all evidence of its presence.<sup>173</sup> This not only helps prevent proliferation, it may be necessary to comply with the legal requirements for time limits on wiretap orders.<sup>174</sup>

¶113 A good example of how non-proliferation might work in practice is demonstrated in a variant of Stuxnet<sup>175</sup> called Gauss. Discovered in August 2012, Gauss appears to be an espionage tool.<sup>176</sup> It uses a known vulnerability and shares some code with other known malware in its dropper, but even after several months of intense analysis, the behavior of its payload remain unknown. Gauss uses cryptographic methods and tools, and only installs and runs on machines specifically targeted by Gauss’s developers; on non-targeted machines it remains encrypted and inert. Gauss also sets up a secure method to send data to its command and control centers. *Ars Technica* reports that “The setup suggests that the command servers handled massive amounts of traffic,”<sup>177</sup> indicating that this technique could send large amounts of data, not just a communications tap.

### G. The Vulnerabilities Market

¶114 One simple way for law enforcement to obtain useful vulnerabilities is to buy them. With the availability of openly published vulnerability information and free exploitation tools, one might question why we discuss purchasing vulnerabilities or exploits from researchers at all. The answer is the improved security of target systems. As software developers and vendors have improved the quality of their software and incorporated defenses such as firewalls and anti-virus packages, vulnerabilities have become harder to find and to exploit. Software companies have also generally accelerated the rate at which they release security patches after critical vulnerabilities have been announced. This can result in a well-patched and well-maintained system more difficult to compromise. Additionally, as stated above, exploits must be carefully tailored to the individual target machine. This means it requires more skill to develop a working exploit, making new effective exploits a valuable commodity for their creator. A technically savvy target, someone who is conscientious about maintaining their system with up-to-date security

---

<sup>173</sup> Fritz Hohl, *Time Limited Blackbox Security: Protecting Mobile Agents from Malicious Hosts*, in MOBILE AGENTS AND SECURITY 90, 97–107 (Giovanni Vigna ed., 1998), available at <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.40.8427>.

<sup>174</sup> See 18 U.S.C. § 2518(4)(e) (2006) (“Each order authorizing or approving the interception of any wire, oral, or electronic communication under this chapter shall specify . . . the period of time during which such interception is authorized . . .”).

<sup>175</sup> See *Stuxnet Dossier*, *supra* note 17.

<sup>176</sup> Dan Goodin, *Nation-Sponsored Malware with Stuxnet Ties has Mystery Warhead*, ARS TECHNICA (Aug. 9, 2012, 1:23 PM), <http://arstechnica.com/security/2012/08/nation-sponsored-malware-has-mystery-warhead/>; KAPERSKY LAB GLOBAL RESEARCH & ANALYSIS TEAM, GAUSS: ABNORMAL DISTRIBUTION, at 21, available at <https://www.securelist.com/en/downloads/vlpdfs/kaspersky-lab-gauss.pdf>, which provides proof of concept despite being an intelligence effort rather than a law enforcement one. The program collects a number of data items, but some of the code is encrypted with a target-specific string. This feature helps prevent proliferation.

<sup>177</sup> Dan Goodin, *Puzzle Box: The Quest to Crack the World’s Most Mysterious Malware Warhead*, ARS TECHNICA (Mar. 14, 2013, 8:00 AM), <http://arstechnica.com/security/2013/03/the-worlds-most-mysterious-potentially-destructive-malware-is-not-stuxnet/>.

patches, is also likely to be careful about not installing software from unverified sources, to use encryption, to not open links from email, and likely does not access questionable websites, and so may not be vulnerable to the easy public exploits. If law enforcement wishes to use a zero-day or lesser-known vulnerability to exploit a target, it must either have the appropriate vulnerability and exploit already on the shelf, or else it must purchase one on the open market. The market itself is a relatively recent phenomenon.

¶115 Finally, there may sometimes be a need to tap a particular suspect as quickly as possible. If there are no suitable off-the-shelf exploits available to the investigators and no time to find a new one, purchasing one may be the best option.<sup>178</sup>

¶116 The overt vulnerabilities marketplace had its start in 2004 when Mozilla launched the first successful bug-bounty program.<sup>179</sup> This program, still in effect today, pays security researchers for original vulnerabilities they discover.<sup>180</sup> Many other companies have followed suit with their own bug-bounty programs. Product developers, however, are not the only groups that are interested in obtaining information regarding software vulnerabilities. Governments and computer security service providers such as iDefense and ZDI also pay for vulnerability information, particularly if the details on how to use it have not been made public (zero-days).<sup>181</sup>

¶117 The overt and black markets in vulnerabilities, exploits, and zero-days have expanded in recent years.<sup>182</sup> Many legitimate security research firms have made finding vulnerabilities and developing exploits for sale part of their business model.<sup>183</sup> Companies and individuals sell information about privately discovered vulnerabilities, often with a proof-of-concept or full-blown exploit code, to groups of subscribers and to individuals. The prices of and amount of detail about the vulnerabilities made public varies. Some companies (e.g., Vulnerability-Lab) and researchers publicly announce that a vulnerability has been discovered in a particular product, but reserve actual details for their customers.<sup>184</sup> Other companies, such as Endgame, keep even the knowledge of the

---

<sup>178</sup> That an exploit has been purchased instead of being developed in-house does not change the need to report it promptly. However, under urgent conditions some delay may be appropriate. *See infra* Section VII.B.

<sup>179</sup> *See* Press Release, Mozilla Found., Mozilla Foundation Announces Security Bug Bounty Program (Aug. 2, 2004), available at <https://www.mozilla.org/en-US/press/mozilla-2004-08-02.html>. For further examples of bug bounties, see Kim Zetter, *With Millions Paid in Hacker Bug Bounties, Is the Internet Any Safer?*, WIRED MAGAZINE (Nov. 8, 2012, 6:30 AM), <http://www.wired.com/threatlevel/2012/11/bug-bounties/all/> (listing prices, total paid out, and launch date for several bug bounty programs).

<sup>180</sup> *See Bug Bounty Program*, MOZILLA, <https://www.mozilla.org/security/bug-bounty.html> (last updated May 22, 2013).

<sup>181</sup> In Feb 2006, iDefense, a vulnerability research company owned by VeriSign, Inc., offered a \$10,000 prize for a ‘previously unknown’ Microsoft security vulnerability. One of the requirements for winning the prize was that the vulnerability be submitted exclusively to iDefense. *See* Brian Krebs, *Wanted: Critical Windows Flaw ... Reward: \$10,000*, SECURITY FIX (Feb. 16, 2006, 1:40 PM), [http://blog.washingtonpost.com/securityfix/2006/02/wanted\\_critical\\_windows\\_flaw\\_r.html](http://blog.washingtonpost.com/securityfix/2006/02/wanted_critical_windows_flaw_r.html).

Similarly, it states in the frequently asked questions for Tipping Point’s Zero Day Initiative that once a vulnerability has been assigned to TippingPoint, it cannot be distributed—or even discussed—elsewhere until a patch is available from the vendor. *See Frequently Asked Questions*, ZERO DAY INITIATIVE, <http://www.zerodayinitiative.com/about/faq/#17.0> (last visited Oct. 7, 2013).

<sup>182</sup> Presumably, if criminals were the only ones interested in purchasing vulnerabilities, the market would still exist, but it would be underground. Similar markets do exist for other forms of criminal software, such as bots, credit card number loggers, etc.

<sup>183</sup> Some prominent examples include: Vupen Security, Vulnerability-Laboratory, Immunity, Inc., Netragard, NSS Labs, Inc., and Raytheon.

<sup>184</sup> Vulnerability Lab posts announcements of vulnerabilities discovered both on its website,

existence of the vulnerability private.<sup>185</sup> Prices range from \$20 to \$250,000,<sup>186</sup> with exclusive access to a critical zero-day generally the most expensive. Recent news reports suggest that national governments, in particular intelligence and military agencies, have become major buyers.<sup>187</sup>

¶118 Companies such as Vupen, Revuln, and Vulnerability-Lab sell subscription services that provide exclusive detailed information on disclosed or private critical vulnerabilities to governments, law enforcement authorities, and corporations.<sup>188</sup> Annual subscriptions can run as high as \$100,000 a year.<sup>189</sup> These companies also sell working exploits and offer special targeted exploit development for additional fees; exploit prices range from \$5,000 to \$250,000. The most valuable are those zero-days that can be used for cyber warfare. For example, the Endgame Systems pricelist includes a twenty-five exploit package for \$2.5 million.<sup>190</sup> Zero-days and exploits can also be purchased from exploit brokers such as Netragard or private brokers who bid on exploits from sellers and negotiate with buyers on behalf of individual exploit developers.<sup>191</sup>

---

<http://www.vulnerability-lab.com>, and on Twitter, [https://twitter.com/vuln\\_lab](https://twitter.com/vuln_lab).

<sup>185</sup> VUPEN Vulnerability Research Team, *Google Chrome Pwned by VUPEN aka Sandbox/ASLR/DEP Bypass*, VUPEN SECURITY (May 9, 2011, 5:35 PM),

[http://www.vupen.com/demos/VUPEN\\_Pwning\\_Chrome.php](http://www.vupen.com/demos/VUPEN_Pwning_Chrome.php) (“For security reasons, the exploit code and technical details of the underlying vulnerabilities will not be publicly disclosed. They are available to our customers as part of our vulnerability research services.”); *Vulnerability Feeds*, REVULN, <http://revuln.com/services.htm#vulnfeeds> (last visited Nov. 13, 2013) (explaining that Revuln sells access to its 0-day Feed, which provides “[i]nformation about undisclosed and unpatched security vulnerabilities found by [their] team in third party hardware and software products of various vendors. The vulnerabilities included in [their] 0-day feed remain undisclosed by ReVuln unless either the vulnerability is discovered and reported by a third party or the vendor publicly or privately patches the issue.”).

<sup>186</sup> Exploits currently offered for public sale from a wide variety of independent researchers can be purchased from <http://exploithub.com>. Further examples of exploits offered for public sale can be found in Andy Greenberg, *Meet the Hackers Who Sell Spies the Tools to Crack Your PC (And Get Paid Six-Figure Fees)*, FORBES (Mar. 21, 2012), <http://www.forbes.com/sites/andygreenberg/2012/03/21/meet-the-hackers-who-sell-spies-the-tools-to-crack-your-pc-and-get-paid-six-figure-fees/>.

<sup>187</sup> See Nicole Perlroth & David E. Sanger, *Nations Buying as Hackers Sell Flaws in Computer Code*, N.Y. TIMES, July 13, 2013, <https://www.nytimes.com/2013/07/14/world/europe/nations-buying-as-hackers-sell-computer-flaws.html>.

<sup>188</sup> See, e.g., VUPEN SECURITY, VUPEN THREAT PROTECTION PROGRAM, *available at* [http://wikileaks.org/spyfiles/files/0/279\\_VUPEN-THREAD-EXPLOITS.pdf](http://wikileaks.org/spyfiles/files/0/279_VUPEN-THREAD-EXPLOITS.pdf) (last visited Nov. 16, 2013).

<sup>189</sup> See Perlroth & Sanger, *supra* note 187.

<sup>190</sup> Michael Riley & Ashlee Vance, *Cyber Weapons: The New Arms Race*, BLOOMBERG BUSINESSWEEK MAG. (July 20, 2011), <http://www.businessweek.com/magazine/cyber-weapons-the-new-arms-race-07212011.html#p4> (quoting David Baker, the vice-president for services at the security firm IOActive, as saying, “‘Endgame is a well-known broker of zero days between the community and the government.’ By ‘community,’ he means hackers—‘Some of the big zero days have ended up in government hands via Endgame . . . .’”).

<sup>191</sup> A number of reports have been published recently documenting the vulnerabilities market and the brokers who negotiate between buyers and sellers. See *The Digital Arms Trade*, THE ECONOMIST (Mar. 30, 2013), <http://www.economist.com/news/business/21574478-market-software-helps-hackers-penetrate-computer-systems-digital-arms-trade>; *Zero Day Exploit Acquisition Program*, NETRAGARD, <http://www.netragard.com/zero-day-exploit-acquisition-program>; Andy Greenberg, *Shopping For Zero-Days: A Price-List for Hackers’ Secret Software Exploits*, FORBES (Mar. 23, 2013, 9:43 AM), <http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/>.

¶119 The FBI has already used vulnerabilities to download exploits and extract information from various targets machines. But if law enforcement uses vulnerabilities and exploits to conduct wiretaps when other methods fail<sup>192</sup> (and as an alternative to CALEA-style taps in the intellectual property world), it will face a difference in scale in the use of such techniques—and thus a difference in kind. That raises not just technical questions, but complex ethical and legal concerns as well. In the sections that follow, we turn to those.

## V. PREVENTING PROLIFERATION

¶120 As should already be clear, the use of an exploit to download a wiretap is far more complex than simply placing two alligator clips on a wire.<sup>193</sup> But what is a far more serious impediment to using exploits is that the exploits employed in the installation of the wiretap may spread beyond the targeted device. Given that possibility, does the government even have the moral right to use vulnerabilities in its efforts to combat crime and protect national security? We consider this issue, and then examine techniques to prevent proliferation of the exploit beyond the intended target.

### A. Public Policy Concerns in Deploying Exploits to Wiretap

¶121 We start with some assumptions. First, there is probable cause that the suspect is committing a serious crime and using the targeted communications device to do so. Second, other means of investigation have been tried and have not netted the requisite information. Third, a wiretap order has been authorized, but the target is using a communications device that prevents the standard methods of interception from working. Is it moral to use an exploit to intercept the communication when there is some risk, however small—but perhaps larger than anticipated—that the exploit may escape the device and be used elsewhere, causing great harm?

¶122 The problem of potentially doing harm in the process of doing good is a well-known problem in philosophy known as “the doctrine of double effect,” in which one pursues a moral action that has a consequence of causing harm. The philosopher Phillipa Foot argued that the distinctions should be between direct intention and oblique action, between avoidance of harm and activities to help,<sup>194</sup> and between duties and voluntary actions. She constructed a series of trenchant examples to illustrate this, including the following:

---

<sup>192</sup> The FBI has said very little about its use of vulnerabilities, let alone why it uses them. Examination of available evidence suggests that their primary reason is when they do not know where the target system is; see, for example, Kevin Poulsen, *FBI Admits it Controlled Tor Servers Behind Mass Malware Attack*, WIRED (Sept. 13, 2013, 4:17 PM), <http://www.wired.com/threatlevel/2013/09/freedom-hosting-fbi/>, which discusses how the FBI used malware to identify child porn viewers who had used Tor. Also note that the FBI would not talk to the press about it, but did talk in court when they had to. See *In Re Warrant to Search a Target Computer at Premises Unknown*, No. H-13-234M, 2013 WL 1729765 (S.D. Tex. Apr. 22, 2013) for an example of such a case.

<sup>193</sup> See *supra* note 20.

<sup>194</sup> PHILLIPA FOOT, VIRTUES AND VICES AND OTHER ESSAYS IN MORAL PHILOSOPHY 19–32 (1978).

- Should a judge who is faced with an angry crowd demanding justice, frame and order the execution of an innocent person to save many others from deaths through rioting?<sup>195</sup>

¶123 Foot observes that the salient issue is not justice, but rather direct versus oblique effects.<sup>196</sup> That is the distinction between what we do (direct intention) and what we allow (oblique action). The judge should not hang an innocent man—direct effect—even if more people die as a result of the rioting that ensues.

¶124 Foot makes a distinction between negative duties—avoidance of harm—and positive duties—bringing aid,<sup>197</sup> as well as between duties and voluntary actions, and concludes that a critical distinction is whether one is bringing aid—a voluntary action—or performing one’s duty.<sup>198</sup> Foot illustrates the issue with another example:

- Should the driver of a runaway tram deliberately aim the tram at one man on the track to stop it or steer the other way, where five men are working and will be killed?<sup>199</sup>

¶125 The driver of the tram is performing a duty and has a responsibility to injure as few people as possible. The driver would be behaving morally in electing to take the track with the single individual.

¶126 In using vulnerabilities to execute wiretaps, law enforcement investigators are performing their required duty of investigating a criminal activity. Under Title III, if a wiretap order is granted this means that evidence is essentially unobtainable in other ways.<sup>200</sup> The duty of investigating the criminal activity may require wiretapping. If the only way to affect the wiretap is through the use of an exploit, then, following the logic presented by Foot regarding duty, this is the way to proceed. *But there must be due diligence to contain the harm.* There are several aspects to containing the harm, including fully vetting necessity and balancing it against the harm that may result and designing the exploit to prevent proliferation beyond the target.<sup>201</sup>

¶127 The law balances competing social goods. For example, the Fourth Amendment balances the social good to society of protecting itself against the social good of protecting individual privacy and security.<sup>202</sup> Law enforcement’s use of vulnerabilities

<sup>195</sup> *Id.* at 23.

<sup>196</sup> *Id.* at 24 (“To choose to execute [an innocent man] is to choose that this evil *shall come about*, and this must therefore count as a *certainty* in weighing up the good and evil involved.”).

<sup>197</sup> *Id.* at 25.

<sup>198</sup> *Id.* at 29.

<sup>199</sup> *Id.* at 23.

<sup>200</sup> Recall that 18 U.S.C. § 2518(3)(c) (2006) requires that “normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.” *But see* United States v. Smith, 893 F.2d 1573, 1582 (9th Cir. 1990) (“Although a wiretap should not be used routinely as the first step in a criminal investigation, it need not be the last resort.”).

<sup>201</sup> There are other harms that may result from using the exploit, such as excessive collection, but these are not substantively different from concerns in “normal” wiretapping efforts. The issue of proliferation is substantively different.

<sup>202</sup> While the usual interpretation of the Fourth Amendment is that it centers on protecting the privacy of the individual against searches by the state, Jed Rubenfeld convincingly argues that the amendment really concerns providing security for individuals against searches by the state. *See* Jed Rubenfeld, *The End of*



can be considered within the same framework of competing social goods. Use of vulnerabilities, at least without reporting them, is not unlike police use of confidential informants (CIs). CIs inform investigations even while aiding criminal activity.

¶128 A common law enforcement tactic is to use a lesser criminal to gather evidence about a higher-up criminal. Within limits, crimes (including further crimes) committed by a “flipped” individual are largely forgiven, so long as that person is providing good evidence against the real target of the investigation. As Daniel J. Castleman, chief of the Investigative Division of the Manhattan district attorney’s office, explained, “With confidential informants we get the benefit of intimate knowledge of criminal schemes by criminals, and that is a very effective way to investigate crime . . . .”<sup>203</sup>

¶129 What happens with wiretaps implemented via exploits is ultimately not very different. In both cases law enforcement seeks to catch what it believes to be a genuinely dangerous criminal. But here it seeks to do so by the collection of wiretap evidence. Installing the tap requires exploiting a vulnerability that law enforcement hopes will not be repaired before the tap is in place.

¶130 The purchase and secret use of vulnerabilities raises several similar moral dilemmas as the use of confidential informants (CIs). The history of police use of CIs is replete with instances where an informant went too far, committing or failing to stop serious criminal activity; this has even included murder.<sup>204</sup> With wiretaps the “too far” is of a somewhat different character, but with similar consequences: some crimes that the government could have stopped may not be prevented. By not reporting the vulnerability to the vendor and speeding its repair, law enforcement’s inactivity is potentially enabling criminal activity against users of the hardware or software. It is thus useful to examine how law views the competing interests of preventing crime versus investigating criminal activity in the use of confidential informants, the closest analogy that exists in practice to the use of unreported vulnerabilities.

¶131 In *United States v. Murphy*, the Seventh Circuit considered a case in which FBI agents created fictitious cases in the Cook County Courts in order to uncover corruption within the legal system.<sup>205</sup> The Seventh Circuit ruled that the false cases were a legitimate investigatory tool, observing that “the phantom cases had no decent place in court. But it is no more decent to make up a phantom business deal and offer to bribe a Member of Congress. In the pursuit of crime the Government is not confined to behavior suitable for the drawing room. It may use decoys, . . . and provide the essential tools of the offense . . . . The creation of opportunities for crime is nasty but necessary business.”<sup>206</sup>

¶132 The choice to use vulnerabilities without also simultaneously reporting them to the vendor is not precisely “the creation of opportunities for crime,” but rather the choice not to pro-actively prevent crime. *Murphy* makes clear that this type of approach can be

---

*Privacy*, 61 STAN. L. REV. 101, 120–38 (2008).

<sup>203</sup> Alan Feuer & Al Baker, *Officers’ Arrest Put Spotlight on Police Use of Informants*, N.Y. TIMES, Jan. 27, 2008, at 26.

<sup>204</sup> There are multiple such examples, including the well-known shooting of Viola Liuzzo, a white supporter of the Civil Rights movement who was shot by Ku Klux Klan members while driving from a march in Selma, Alabama, one of whom was an FBI informant. DIANE MCWHORTER, CARRY ME HOME: BIRMINGHAM, ALABAMA: THE CLIMACTIC BATTLE OF THE CIVIL RIGHTS REVOLUTION 572–73 (2001).

<sup>205</sup> 768 F.2d 1518, 1524 (7th Cir. 1985).

<sup>206</sup> *Id.* at 1529.

legally legitimate. Whether it is acceptable is a moral, public policy, and political question.

¶133 Department of Justice guidelines on the use of confidential informants state that a Justice Law Enforcement Agent (JLEA) is never permitted to authorize a CI to “participate in an act of violence; . . . participate in an act that constitutes obstruction of justice (e.g., perjury, witness tampering, witness intimidation, entrapment, or the fabrication, alteration, or destruction of evidence); . . . participate in an act designed to obtain information for the JLEA that would be unlawful if conducted by a law enforcement agent (e.g., breaking and entering, illegal wiretapping, illegal opening or tampering with the mail, or trespass amounting to an illegal search); or . . . initiate or instigate a plan or strategy to commit a federal, state, or local offense.”<sup>207</sup> The guidelines do not state, however, that a CI *must* work to prevent a crime from occurring. The analogous situation to the use of vulnerabilities would be that law enforcement is not required to let vendors know about the vulnerabilities they find and exploit.

¶134 Immediately reporting versus using for some time before reporting is a clash of competing social goods, which is what we need to weigh here. If our primary concern is preventing the proliferation of exploits, society will be better protected by reporting the vulnerability early even if that risks the ability of the criminal investigation to conduct its authorized wiretap.

¶135 As we know from other situations, whether rare diseases or the effect of cold weather on shuttle O-rings,<sup>208</sup> a rare side effect is more likely to appear when working with a large population sample. The danger of proliferation means each use of an exploit, even if it has previously run successfully, increases the risk that the exploit will escape the targeted device. This introduces a serious wrinkle in the use of vulnerabilities, one that law enforcement must address, and that we discuss in subsection C and section VI, *supra*.

### B. Ethical Concerns of Exploiting Vulnerabilities to Wiretap

¶136 Even though wiretaps have long been accepted as a tool in law enforcement’s toolbox, there is something distasteful about using an exploit to download interception capability. Undoubtedly, part of that distaste stems from the strong sense that vulnerabilities are to be patched, not exploited. But even if law enforcement were never to report the vulnerabilities it discovers or purchases, law enforcement’s use of vulnerabilities would not make the vulnerability situation worse. Law enforcement does not currently report vulnerabilities to vendors. Thus, were law enforcement to use vulnerabilities and not report them to the vendors, there would be no change to the status quo ante. That said, there are still some concerns raised by law enforcement’s use of vulnerabilities.

---

<sup>207</sup> Illegal activity must be authorized in advance for a period of up to ninety days. See DEP’T OF JUSTICE, DEPARTMENT OF JUSTICE GUIDELINES REGARDING THE USE OF CONFIDENTIAL INFORMANTS (Jan. 8, 2001), <http://www.justice.gov/ag/readingroom/ciguide.htm>.

<sup>208</sup> Howard Berkes, *Reporting a Disaster’s Cold, Hard Facts*, NPR (Jan. 28, 2006, 1:27 PM), <http://www.npr.org/templates/story/story.php?storyId=5175151>.

¶137 One danger of law enforcement's participation in the zero-day market is the possibility of skewing the market, either by increasing incentives against disclosure of the vulnerability or by increasing the market for vulnerabilities and thus encouraging greater participation in it. Because of the current size of the market and the relatively minimal need by law enforcement, we do not believe that this will be an issue. It is hard to know exactly under which circumstances vulnerabilities will be used since the FBI has not discussed under what technical circumstances they have encountered difficulties wiretapping, but we do believe usage will be rare.

¶138 What is the government's responsibility in cases where the operationalized vulnerability escapes the target? It is not unheard of for physical searches to go amiss; sometimes law enforcement executes a warrant on the wrong location or executes a wiretap warrant on the wrong phone line.<sup>209</sup> Such a search would, of course, invalidate collection. But a wiretap exercised through an operationalized payload is a significantly different situation. Unlike an incorrectly executed wiretap warrant, which might simply collect information on the wrong party, a badly designed payload could escape its target and potentially affect a much larger group of people.

¶139 If the operationalized vulnerability were to escape its target, it might be adapted for malicious purposes by others, a second-order affect that increases the need for great care in developing the exploits. While the government may have some liability when it knocks down the wrong door in the course of exercising a search warrant,<sup>210</sup> with wiretap software the liability—in dollars or simply in costs to society—is not as well understood.

¶140 As a result, it is critical that the tools employed by law enforcement be trustworthy and reliable. In particular, the technical implementation must capture only what is authorized. In addition, all the usual security provisions apply: the system must employ full auditing of actions taken or system changes made,<sup>211</sup> each user of the system must log on individually, etc.<sup>212</sup> Such careful controls have not always been exercised in the past, as is evidenced by flaws discovered in the FBI's DCS 3000 wiretap system,<sup>213</sup> as well as poor documentation of telephone transactional data requests during FBI investigations post-September 11th.<sup>214</sup> This argues for not only judicial oversight, but technical oversight as well.

---

<sup>209</sup> See, e.g., INTELLIGENCE OVERSIGHT BOARD MATTER, [REDACTED] DIVISION, FEDERAL BUREAU OF INVESTIGATION HEADQUARTERS, IOB MATTER 2005-160 (June 30, 2010), available at [https://www.eff.org/sites/default/files/filenode/intel\\_oversight/IOB%202005-160.pdf](https://www.eff.org/sites/default/files/filenode/intel_oversight/IOB%202005-160.pdf). It is rare that such activity is publicly reported. *Documents Obtained by EFF Reveal FBI Patriot Act Abuses*, ELECTRONIC FRONTIER FOUNDATION (Mar. 31, 2011), <https://www.eff.org/deeplinks/2011/03/documents-obtained-eff-reveal-fbi-patriot-act>.

<sup>210</sup> Cf. Jim Armstrong, *FBI Uses Chainsaw in Raid on Wrong Fitchburg Apartment*, CBS BOSTON (Jan. 31, 2012, 11:59 PM), <http://boston.cbslocal.com/2012/01/31/fbi-uses-chainsaw-in-raid-on-wrong-fitchburg-apartment/>.

<sup>211</sup> This was missing in the Greek wiretapping case. See Prevelakis & Spinellis, *supra* note 4.

<sup>212</sup> There are many commercial and government guides to operating secure computer systems. See, e.g., *Operating Systems*, NAT'L SECURITY AGENCY, [http://www.nsa.gov/ia/mitigation\\_guidance/security\\_configuration\\_guides/operating\\_systems.shtml](http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml) (last updated Aug. 14, 2013).

<sup>213</sup> The system was previously known as Carnivore. See Steven M. Bellovin, Matt Blaze, David Farber, Peter Neumann & Eugene Spafford, *Comments on the Carnivore System Technical Review* (Dec. 3, 2000), [http://www.crypto.com/papers/carnivore\\_report\\_comments.html](http://www.crypto.com/papers/carnivore_report_comments.html).

<sup>214</sup> U.S. DEP'T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S USE OF EXIGENT LETTERS AND OTHER INFORMAL REQUESTS FOR TELEPHONE RECORDS 46–47, 70 (Jan. 2010), available at

¶141 Finally, one might imagine a scenario in which law enforcement puts pressure on vendors not to fix vulnerabilities so as to facilitate exploits. Aside from being bad public policy, such an approach would be dangerous for both government and industry. If such pressure became publicly known, the vendor would suffer serious reputational harm. It is not inconceivable that the vendor could also be liable to customers for damages if the company knew of a serious vulnerability about which it had neither informed its customers nor patched to eliminate the vulnerability.<sup>215</sup>

### C. Technical Solutions to Preventing Proliferation

¶142 The principle of only harming the target must govern the use of vulnerabilities by law enforcement. One means of ensuring that only the target is harmed is to employ technical mechanisms to restrict an exploit to a given target machine. The simplest mechanisms check various elements of their environment when they run, e.g., the machine's serial number or MAC address, and if they are on the wrong machine silently exit. Stuxnet employed this technique.<sup>216</sup> A more sophisticated technique is to use environmental data to construct a cryptographic key; if this data is not present, a key cannot be constructed and the data will not decrypt properly, and the code will not be comprehensible to any analyst. Gauss malware uses this technique, and has stymied top cryptanalysts for months.<sup>217</sup>

¶143 From one perspective, the part of the exploit that contains the vulnerability is the most important piece, since knowledge of it will let people write their own exploit code. The best defense against this is to use a dropper/payload architecture; that way, after the initial penetration there is no further need for the vulnerability and the code relying on it can be deleted.<sup>218</sup>

¶144 Promiscuous spread of penetration tools also increases the risk of proliferation. The more machines a piece of code is on, the more likely it is that someone will notice the code and reverse-engineer it. This would expose not just a carefully husbanded vulnerability, but also the surrounding infrastructure necessary to use it for lawful intercepts. This calculus is similar to one found in the intelligence community: if one acts on intelligence, one risks giving away the source of information, which would then be unavailable in the future.<sup>219</sup>

---

[https://www.eff.org/sites/default/files/filenode/intel\\_oversight/IOB%202005-160.pdf](https://www.eff.org/sites/default/files/filenode/intel_oversight/IOB%202005-160.pdf).

<sup>215</sup> Current law (such as UCC Article 2) and the wording of end-user license agreements (EULAs) make this outcome unlikely. Note, though, that some computer worms have affected people who were not parties to these agreements: the worms' spread clogged the Internet sufficiently that other people could not use it. See generally Jane Chong, *We Need Strict Laws if We Want More Secure Software*, New Republic (Oct. 30, 2013), <http://www.newrepublic.com/article/115402/sad-state-software-liability-law-bad-code-part-4>.

<sup>216</sup> See *Stuxnet Dossier*, *supra* footnote 17.

<sup>217</sup> See *supra* notes 176–78 and accompanying text.

<sup>218</sup> The best analogy to a “dropper” is a lock pick. Once you've unlocked the door—i.e., once the dropper has used a vulnerability to penetrate the system—you no longer need the lock pick; you can move around freely inside the house. You can even open the door again, from the inside, to bring in new materials, i.e., the “payload.”

<sup>219</sup> See DAVID KAHN, *THE CODE-BREAKERS* (1967). The theme that if one acts on intelligence, one risks giving away the source of the information, which will then be unavailable in the future pervades the book, but the discussion of the assassination of Admiral Isoroku Yamamoto on pgs. 595–601 is especially illustrative.

## VI. REPORTING VULNERABILITIES

¶145 The CIPAV cases<sup>220</sup> demonstrate that the state employs vulnerabilities for searches<sup>221</sup>—the “can” problem—so we turn to the “may” problem: namely, may law enforcement do so?<sup>222</sup> We have already argued that the security risks that would be created by extending CALEA to IP-based communications make it a poor choice. In contrast, if the vulnerability being used to introduce a wiretap already exists, the issue is somewhat different, and the question instead concerns patching. If a vulnerability in a communications application or infrastructure is patched, the vulnerability cannot be exploited for a wiretap. But if the vulnerability is left unpatched, the result is that many are left open to attack. Thus the issue is not about introducing an exploit, but about when, and perhaps whether, to inform the vendor of the vulnerability.

¶146 What is law enforcement’s responsibility with regard to reporting? We start by examining the security risks created by using vulnerabilities, then consider that risk in the context of law enforcement’s role in crime prevention.

*A. Security Risks Created by Using Vulnerabilities*

¶147 As we have already noted in Section V, there is a danger that even the most carefully crafted exploitation tools may not function as intended. There are at least three security concerns that must be weighed in choosing to use a vulnerability to conduct a wiretap: (i) the risk that the vulnerability’s use will lead to overcollection, (ii) the danger that the penetration tools may have unintended side effects on the targeted system, and (iii) the danger that the vulnerability will accidentally escape its target device and find use elsewhere. (This latter point is discussed in Section V.C, *supra*.)

¶148 Unfortunately there is much precedent for overcollection. Recent examples include the NSA’s overcollection<sup>223</sup> as a result of the FISA Amendments Act<sup>224</sup> and the FBI’s use of “exigent” letters to collect communications transactional data.<sup>225</sup> Use of the vulnerabilities requires close scrutiny by judges to ensure that what is collected is only what is authorized to be collected. Judges will therefore need to evaluate just how intrusive a particular exploit may be, a technical as well as legal issue.

¶149 The wiretap statute requires that taps be done “with a minimum of interference” with the service being monitored.<sup>226</sup> If an exploit causes other harm to the target computer, such as damaging files or applications or leading to frequent crashes, use of the

---

<sup>220</sup> See *supra* notes 132–33 and accompanying text.

<sup>221</sup> See Lynch, *supra* note 133.

<sup>222</sup> We are indebted to Marty Stansell-Gamm for the phrasing of the “may” versus “can” problem.

<sup>223</sup> A major concern was that the collection inappropriately included communications of Americans without particularized FISA warrants. See, e.g., James Risen & Eric Lichtblau, *Extent of E-Mail Surveillance Renews Concern in Congress*, N. Y. TIMES, June 16, 2009, at A1.

<sup>224</sup> Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783, *as amended by* Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. 110-261, 122 Stat. 2436.

<sup>225</sup> The multiple problems included: (i) many of the exigent letters never received proper follow-up by National Security Letters, (ii) sometimes private subscriber data was given to the FBI without a written request, (iii) many of the exigent letter requests failed to specify a date, thus leading to a response that included information well outside the intended investigatory period, (iv) many of the requests were not related to an actual emergency, etc. See U.S. DEP’T OF JUSTICE, *supra* note 214, at 257–72.

<sup>226</sup> 18 U.S.C. § 2518(4) (2006).

exploit would violate this provision. At least one court has already quashed an eavesdropping order on these grounds:

Looking at the language of the statute, the “a minimum of interference” requirement certainly allows for *some* level of interference with customers’ service in the conducting of surveillance. We need not decide precisely how much interference is permitted. “A minimum of interference” at least precludes total incapacitation of a service while interception is in progress. Put another way, eavesdropping is not performed with “a minimum of interference” if a service is *completely* shut down as a result of the surveillance.<sup>227</sup>

¶150 It is worth noting that in this case, there were no allegations of instances of the customer trying and failing to use the service; however, use of the wiretap would make the original service unavailable to the customer if requested.<sup>228</sup>

¶151 Apart from legal considerations, it is worth noting that interference can lead to discovery of the tap. This has happened at least twice in what appear to have been intelligence operations. During a very sophisticated wiretap operation mounted against a Greek cellphone operator, a bug in the attacking software caused some text messages not to be delivered. The resulting error messages led to discovery of the implanted code.<sup>229</sup> In a better-known case, the Stuxnet virus aimed at the Iranian nuclear centrifuge plant was discovered when a computer user became suspicious and sent a computer to a Belarusian antivirus firm for analysis.<sup>230</sup>

### B. Preventing Crime

¶152 The question of when to report vulnerabilities that are being exploited is not new for the U.S. government. In particular, the National Security Agency (NSA) has faced this issue several times in its history, as we discuss below.

¶153 The NSA performs two missions for the U.S. government: the well-known mission of signals intelligence, or SIGINT, which involves “reading other people’s mail,”<sup>231</sup> and the lesser-known mission of communications security, COMSEC, which involves protecting U.S. military and diplomatic communications.<sup>232</sup> In principle, it is extremely useful to house the U.S. signals intelligence mission in the same agency as the U.S. communications security mission because each is in a position to learn from the other. SIGINT’s ability to penetrate certain communication channels could inform COMSEC’s

---

<sup>227</sup> *Company v. United States*, 349 F.3d 1132, 1145 (9th Cir. 2002) (internal citations omitted).

<sup>228</sup> *Id.* at 1134–35.

<sup>229</sup> See Prevelakis & Spinellis, *supra* note 4.

<sup>230</sup> See John Borland, *A Four-Day Dive Into Stuxnet’s Heart*, WIRED (Dec. 27, 2010, 8:27 PM), <http://www.wired.com/threatlevel/2010/12/a-four-day-dive-into-stuxnets-heart/>.

<sup>231</sup> Henry Stinson, the Secretary of State who shut down the “Black Chamber,” the Army’s signals intelligence section during and after World War I, famously said, “Gentlemen do not read each other’s mail.” His views changed during World War II when he was Secretary of War; the U.S. relied heavily on signals intelligence during that conflict. Though the quote is attributed to Stinson, there is some evidence that he was acting on President Hoover’s orders. See DAVID KAHN, *THE READER OF GENTLEMEN’S MAIL: HERBERT O. YARDLEY AND THE BIRTH OF AMERICAN CODEBREAKING* (2004).

<sup>232</sup> The COMSEC mission is performed by the NSA’s Information Assurance Division.

knowledge of potential weaknesses in our own and COMSEC's awareness of security problems in certain communications channels might inform SIGINT's knowledge of a target's potential weakness.

¶154 Reality is in fact very different. COMSEC's awareness of the need to secure certain communications channels has often been thwarted by SIGINT's desire that patching be delayed so that it can continue to exploit traffic using the vulnerability in question. How this contradictory situation is handled depends primarily on where the vulnerable communications system is operating. If the insecure communications system is being used largely in the U.S. and in smaller nations that are unlikely to harm the U.S., then patching would not hurt the SIGINT mission. In that situation, COMSEC is allowed to inform the vendor of the vulnerability. In most other instances, informing the vendor is delayed so that SIGINT can continue harvesting product. Although this was never a publicly stated NSA policy, this modus operandi was a fairly open secret.<sup>233</sup>

¶155 Law enforcement operates in a different domain than the military, so its considerations and values are different. The FBI's concern that it is "going dark" is in regard to domestic wiretapping; law enforcement wants to exploit the vulnerabilities *exactly* when there are users in the U.S. Thus the balancing that NSA does between its SIGINT and COMSEC missions does not particularly illuminate what the state of affairs should be for the FBI. We must instead examine the issue from other vantage points.

¶156 One criterion that law enforcement should use is the likelihood of collateral damage from using vulnerabilities. By their nature some vulnerabilities are easier to exploit than others. More critically, some vulnerabilities are likely to be easier for law enforcement to exploit than for the general population of attackers to do so. Any attack that is aided by the ability to use compulsory legal process against a third party, such as an ISP, falls into this category. In these cases, failure to report the vulnerability to the vendor is less likely to have an effect on its exploitation by others.

¶157 There are also other factors that can make launching an exploit complicated, like needing knowledge of special information or material about the target. If possession of such knowledge or information is necessary for the vulnerability to be exploited, then law enforcement can be fairly confident that there is little risk in not reporting the vulnerability to the vendor.

¶158 In considering whether to report a vulnerability, law enforcement should consider how dangerous a particular vulnerability may be. Sometimes this question will be very easy to answer. If the vulnerability is in a network router or a switch, its impact is likely to be very large. Indeed, vulnerabilities in network infrastructure are fundamentally a national security risk because network devices are either ISP-grade gear, whose compromise could be used to shut down or tap a large portion of the network; enterprise gear, whose compromise could be used for targeted espionage attacks; or consumer gear, likely to be in wide use and thus the compromise could effect a large population. Without question, such vulnerabilities should be reported to the vendor immediately.

¶159 There are subtleties involved even if a vulnerability does not initially appear to be one that could create a national security risk. If the vulnerability is for an uncommon platform, it would seem that not informing the vendor of the problem is unlikely to create much risk. If the vulnerability is for an outdated version of a platform, depending on how

---

<sup>233</sup> Interview with redacted source, Feb. 24, 2013, on file with author Susan Landau.

outdated the platform is, the risk may also be relatively minor.<sup>234</sup> The latter is especially true for devices that are replaced frequently, e.g., smart phones. Yet it is often the case that outdated systems may be widely deployed in non-critical systems or even deployed in critical systems,<sup>235</sup> so that a vulnerability that exists in an outdated version of a platform may still be widely dangerous; it depends on exactly on who is using the platform and in what situation. This demonstrates the complexity of determining when the vendor should be told about the vulnerability.

¶160 This raises the concern of whether the FBI will actually be able make an evaluation of whether a vendor should be informed of a vulnerability. As the examples above show, the ability to discern the potential risk from any particular vulnerability ranges from relatively trivial to quite difficult. One limitation on the FBI's ability to make an evaluation is that the Domestic Communications Assistance Center (DCAC) does not have the expertise to be a cybersecurity vulnerability research center.<sup>236</sup> Nor should it have; that expertise lies with the NSA's Information Assurance Directorate, and duplicating the expertise is neither possible nor appropriate. Making such evaluations requires vast knowledge about systems being employed in the U.S. across a wide array of industries. Even a decade after September 11th, this information is not being tracked by the U.S. government. The FBI is certainly not in a position to know this information, or to be able to make the determination about how dangerous to the U.S. a particular vulnerability may be.

¶161 The point is that except for some obvious cases, it is usually very difficult to determine a priori whether a particular vulnerability is likely to create a serious problem.<sup>237</sup> It could be that some obscure, but critical part of society relies on the code with the vulnerability. It could also be that it lies in some hidden part of the nation's critical infrastructure; for example, for decades American Airlines relied on old software for planning flight operations.<sup>238</sup> Furthermore—and especially in an open-source world,

---

<sup>234</sup> This issue makes for an interesting insight into pirated software. The fact that a high percentage of software in China is illegally obtained has several implications for electronic surveillance. The most significant implication is probably that the versions are not only out of date—e.g., as of January 2013, 62% of Chinese Windows users had Windows XP installed, while 32% had Windows 7, *StatCounter Global Stats: Top 7 Operating Systems in China from Feb 2012 to Jan 2013*, <http://gs.statcounter.com/#os-CN-monthly-201202-201301> (last visited Feb. 17, 2013)—but also that they are less secure than more modern systems. Thus, they are more open to exploitation.

<sup>235</sup> One example of this is Windows XP; the eleven-year-old OS is still the most common operating system in use at most government agencies. Shawn McCarthy, *8 Reasons Agency IT Will Change Course in 2013*, GCN (Nov. 16, 2012) <http://gcn.com/articles/2012/11/16/8-reasons-agency-it-will-change-course-in-2013.aspx>. Another is the backend system supporting voting machines in Ohio. PATRICK MCDANIEL ET AL., EVEREST: EVALUATION AND TESTING OF ELECTION-RELATED EQUIPMENT, STANDARDS, AND TESTING (Dec. 7, 2007), *available at* <http://www.sos.state.oh.us/SOS/upload/everest/14-AcademicFinalEVERESTReport.pdf>

<sup>236</sup> See McCullagh, *supra* note 167.

<sup>237</sup> A striking example of an obviously dangerous vulnerability occurred with the February 2013 US-CERT alert concerning Java; the organization recommended disabling Java in web browsers until an adequate patch had been prepared. *Alert (TA13-032A): Oracle Java Multiple Vulnerabilities*, US-CERT (Feb. 1, 2013), <https://www.us-cert.gov/ncas/alerts/TA13-032A>.

<sup>238</sup> Robert L. Mitchell & Johanna Ambrosio, *From Build to Buy: American Airlines Changes Modernization Course Midflight*, COMPUTERWORLD (Jan. 2, 2013), [https://www.computerworld.com/s/article/9234936/From\\_build\\_to\\_buy\\_American\\_Airlines\\_changes\\_modernization\\_course\\_midflight\\_](https://www.computerworld.com/s/article/9234936/From_build_to_buy_American_Airlines_changes_modernization_course_midflight_).



where it may be impossible to determine all the users of a system—there is no way that law enforcement would be in a position to do a full mapping from software to users, because there is no way to tell whom they all are.

¶162

As we alluded to earlier, this is a clash of competing social goods between the security obtained by patching as quickly as possible and the security obtained by downloading the exploit to enable the wiretap to convict the criminal. Although there are no easy answers, we believe the answer is clear. In a world of great cybersecurity risk, where each day brings a new headline of the potential for attacks on critical infrastructure,<sup>239</sup> where the Deputy Secretary of Defense says that thefts of intellectual property “may be the most significant cyberthreat that the United States will face over the long term,”<sup>240</sup> public safety and national security are too critical to take risks and leave vulnerabilities unreported and unpatched. We believe that law enforcement should always err on the side of caution in deciding whether to refrain from informing a vendor of a vulnerability. Any policy short of full and immediate reporting is simply inadequate. “Report immediately” is the policy that any crime-prevention agency should have, even though such an approach will occasionally hamper an investigation.<sup>241</sup>

¶163

Note that a report immediately policy does not foreclose exploitation of the reported vulnerability by law enforcement. Vulnerabilities reported to vendors do not result in immediate patches; the time to patch varies with each vendor’s patch release schedule (once per month, or once every six weeks is common), but, since vendors often delay patches,<sup>242</sup> the lifetime of a vulnerability is often much longer. Research shows that the average lifetime of a zero-day exploit is 312 days.<sup>243</sup> Furthermore, users frequently do not patch their systems promptly, even when critical updates are available.<sup>244</sup>

---

<sup>239</sup> See, e.g., Kim Zetter, *Researchers Uncover Holes That Open Power Stations to Hacking*, WIRED (Oct. 16, 2013, 12:00 PM), <http://www.wired.com/threatlevel/2013/10/ics/>.

<sup>240</sup> William J. Lynn III, *Defending a New Domain*, 89 FOREIGN AFF. 97, 100 (2010).

<sup>241</sup> There are persistent rumors that government agencies have sometimes pressured vendors to leave holes unpatched. See, e.g., Graeme Burton, *Microsoft Gives Zero-Day Vulnerabilities to US Security Services - Bloomberg*, COMPUTING (June 14, 2013), <http://www.computing.co.uk/ctg/news/2274993/microsoft-gives-zero-day-vulnerabilities-to-us-security-services-bloomberg>. This is a very dangerous path, one that should not be followed by law enforcement agencies.

<sup>242</sup> On the second Tuesday of every month, Microsoft issues patches both for software defects and vulnerabilities. This date is known as “Patch Tuesday.” Vendors who use a 6-week “rapid-release cycle,” such as Google (Chrome) and Mozilla (Firefox, Thunderbird), frequently roll their security patches into their new releases. However, not all vulnerabilities discovered are patched in the next release. See, e.g., Tony Bradley, *Patch Tuesday Leaves Internet Explorer Zero Day Untouched*, PC WORLD (Apr. 9, 2013, 12:55 PM), <http://www.pcworld.com/article/2033649/patch-tuesday-leaves-internet-explorer-zero-day-untouched.html>; Michael Mimoso, *Oracle Leaves Fix for Java SE Zero Day Until February Patch Update*, THREATPOST (Oct. 17, 2012, 2:41 PM), <http://threatpost.com/oracle-leaves-fix-java-se-zero-day-until-february-patch-update-101712/>. Some vendors do issue patches considerably more rapidly; it is unclear, though, that this is always a good idea. Rapid patches often block a particular path to reach the underlying buggy code rather than repairing it. Accordingly, attackers often find new variants of the exploit without much trouble. Sometimes patches contain their own flaws. Thus, there is likely an irreducible average minimum time.

<sup>243</sup> Zero-day vulnerabilities average a 10-month lifespan. Leyla Bilge & Tudor Dumitras, *Before we Knew It: An Empirical Study of Zero-day Attacks in The Real World*, PROC. 2012 ACM CONF. ON COMPUTER & COMM. SECURITY 833, 834 (2012).

<sup>244</sup> There is a paucity of peer-reviewed research results on how soon individual users apply patches. The best studies are old and apply to enterprise servers, not individual users. See, e.g., Eric Rescorla, *Security Holes... Who Cares?*, PROC. 12TH USENIX SECURITY SYMP. 75, 75 (2003); CHESWICK, BELLOVIN & RUBIN, *supra* note 151, at 74–75. Enterprises have their own needs and dynamics for patching, such as

¶164 Immediate reporting to the vendor of vulnerabilities considered critical will result in a shortened lifetime for particular operationalized exploits, but it will not prevent the use of operationalized exploits. Instead, it will create a situation in which law enforcement is both performing criminal investigations using the wiretaps enabled through the exploits, and crime prevention through reporting the exploits to the vendor. This is clearly a win/win situation.

¶165 It is interesting to ponder whether the policy of immediately reporting vulnerabilities could disrupt the zero-day industry. Some members of the industry, such as HP DVLabs, “will responsibly and promptly notify the appropriate product vendor of a security flaw with their product(s) or service(s).”<sup>245</sup> Others, such as VUPEN, which “reports all discovered vulnerabilities to the affected vendors under contract with VUPEN,”<sup>246</sup> do not. Although it would be a great benefit to security if the inability to sell to law enforcement caused the sellers to actually change their course of action, U.S. law enforcement is unlikely to have a major impact on the zero-day market since it is an international market dominated by national security organizations.

---

concerns about compatibility with critical local software; furthermore, all system administration is generally under the control of a centralized support group. Most wiretaps are of individuals, especially drug dealers. *See* ADMIN. OFFICE OF THE U.S. COURTS, *supra* note 53. Therefore, their behavior is likely very different. There have been a number of statements by industry consistent with our assertion. *See, e.g.*, Press Release, Skype, Survey Finds Nearly Half of Consumers Fail to Upgrade Software Regularly and One Quarter of Consumers Don’t Know Why to Update Software (July 23, 2012), *available at* [http://about.skype.com/press/2012/07/survey\\_finds\\_nearly\\_half\\_fail\\_to\\_upgrade.html](http://about.skype.com/press/2012/07/survey_finds_nearly_half_fail_to_upgrade.html). A recent study is useful, since it measures actual exposure of real-world web browsers. *How are Java Attacks Getting Through?*, WEBSense (Mar. 25, 2013, 9:01 PM), <http://community.websense.com/blogs/securitylabs/archive/2013/03/25/how-are-java-attacks-getting-through.aspx>. Only about 5% of users had up-to-date Java versions, despite warnings of ongoing attacks. *Id.* The best evidence, though, is empirical: the prevalence of attacks against holes for which patches are available suggests that attackers still find them useful.

<sup>245</sup> *See Disclosure Policy*, ZERO DAY INITIATIVE, [http://www.zerodayinitiative.com/advisories/disclosure\\_policy/](http://www.zerodayinitiative.com/advisories/disclosure_policy/) (last visited Mar. 1, 2013). It goes on to say:

The first attempt at contact will be through any appropriate contacts or formal mechanisms listed on the vendor Web site, or by sending an e-mail to security@, support@, info@, and secure@company.com with the pertinent information about the vulnerability. Simultaneous with the vendor being notified, DVLabs may distribute vulnerability protection filters to its customers' IPS devices through the Digital Vaccine service.

If a vendor fails to acknowledge DVLabs initial notification within five business days, DVLabs will initiate a second formal contact by a direct telephone call to a representative for that vendor. If a vendor fails to respond after an additional five business days following the second notification, DVLabs may rely on an intermediary to try to establish contact with the vendor. If DVLabs exhausts all reasonable means in order to contact a vendor, then DVLabs may issue a public advisory disclosing its findings fifteen business days after the initial contact.

*Id.*  
<sup>246</sup> *Vupen Security Research Team – Discovered Vulnerabilities in Prominent Software*, VUPEN SECURITY, <http://www.vupen.com/english/research-vuln.php> (last viewed Mar. 1, 2013) (emphasis added).

### C. A Default Obligation to Report

¶166 The tension between exploitation and reporting can be resolved if the government follows *both* paths, actively reporting and working to fix even those vulnerabilities that it uses to support wiretaps. As we noted, the reporting of vulnerabilities (to vendors and/or to the public) does not preclude exploiting them.<sup>247</sup> Once a vulnerability is reported, there is always a lead time before a “patch” can be engineered, and a further lead time before this patch is deployed to and installed by future wiretap targets. Because there is an effectively infinite supply of vulnerabilities in software platforms,<sup>248</sup> provided new vulnerabilities are found at a rate that exceeds the rate at which they are repaired, reporting vulnerabilities need not compromise the government’s ability to conduct exploits. By always reporting, the government investigative mission is not placed in conflict with its crime prevention mission. In fact, such a policy has the almost paradoxical affect that the more active the law enforcement exploitation activity becomes, the more zero-day vulnerabilities are reported to and repaired by vendors.

¶167 However, this does not mean that a law enforcement exploitation laboratory will be naturally inclined to report the fruits of its labor to vendors. From the perspective of an organization charged with developing exploits, reporting might seem an anathema to the mission, since it means that the tools it develops will become obsolete more quickly. Discovering and developing exploits costs money, and an activity that requires more output would need a larger budget.<sup>249</sup>

¶168 An obligation mandating that law enforcement agencies report any zero-day vulnerabilities they intend to exploit should thus be supported by a strong legal framework. Such a framework should create bright lines for what constitutes a vulnerability that must be reported, when the reporting must occur, to whom the report should be made, and which parts of the government are required to do the reporting. There are many grey areas.

¶169 First, what should constitute a reportable vulnerability? Sometimes, this will be obvious. For example, some software bugs, such as input validation errors, might allow an attacker to take control over a piece of software.<sup>250</sup> Such behavior is clearly an error. Once reported, the software vendor can easily repair the software to eliminate the vulnerability and “push” the patch out.<sup>251</sup> Other vulnerabilities are less clearly the result of specific bugs, however. Sometimes, a vulnerability results from overly powerful software features that are behaving perfectly correct as far as the software specification is concerned, but that allow an attacker to exploit them in unanticipated ways. For example, many email systems allow software to be sent as an “attachment” that is executed on the

---

<sup>247</sup> The question of publicly disclosing vulnerabilities is at the core of a very involved debate. The two basic positions are “responsible disclosure”, i.e., only to the vendor for a reasonable period (typically a few months) or “full disclosure”. Without going into details, the argument for full disclosure is threefold: first, it has often been necessary to force the vendor to act; second, people have a right to know what risks they’re being exposed to (think of food labeling laws and many other product disclaimers); three, it lets individuals and companies act to protect themselves until a vendor fix is available.

<sup>248</sup> See BROOKS, *supra* note 116.

<sup>249</sup> It is difficult to estimate precisely the cost of developing a particular vulnerability, but existing markets can serve as a guide here, as discussed in Section IV.

<sup>250</sup> See, e.g., *supra* note 98.

<sup>251</sup> Many companies, if not most, provide automatic security updates that are simply updated via the Internet.

recipient's computer when the user clicks on it. If an attacker emails a user malware and the user is persuaded, however unwisely, to open it, the user's computer becomes compromised. Although it served as a vector for the malware, the email system software, strictly speaking, has behaved correctly here. The line between a "bug" and a "feature" is often quite thin.

¶170 Then there is the question of when a potential vulnerability that has been discovered becomes "reportable." Many vulnerabilities result from subtle interactions in a particular implementation,<sup>252</sup> and not every software bug results in an actual exploitable vulnerability. If the government is obligated to report exploitable vulnerabilities, when must it do so? An appropriate guideline would be that once the government has developed an exploit tool, the underlying vulnerability has been confirmed to be exploitable and should promptly be reported. Note that this way of implementing the always report policy gives law enforcement investigators some lead-time in using the exploit tool. This approach provides appropriate leeway for law enforcement to do its job by exploiting these vulnerabilities, while not making them quality assurance testers for software companies.

¶171 To whom should a vulnerability report be made? In many cases, there is an obvious point of contact: a software vendor that sells and maintains the product in question, or, in the case of open-source software, the community team maintaining it. In other cases, however, the answer is less clear. Not all software is actively maintained; there may be "orphan" software without an active vendor or owner to report to.<sup>253</sup> Also, not all vulnerabilities result from bugs in specific software products. For example, standard communications protocols are occasionally found to have vulnerabilities,<sup>254</sup> and a given protocol may be used in many different products and systems. In this situation, the vulnerability would need to be reported not to a particular vendor, but to the standards body responsible for the protocol. Many standards bodies operate entirely in the open,<sup>255</sup> however, which can make quietly reporting a vulnerability—or hiding the fact that it has been reported by a law enforcement agency—problematic. In this situation, the choice is simple: report it openly.

---

<sup>252</sup> Quite some time ago, one of the authors of this paper discovered that someone working on an important project was one of three people arrested in a hacking incident. (He eventually pled no contest. One of the other two was convicted; the third was acquitted.) An audit of the code base was performed. The team found one clear security hole, but log files showed it was an inadvertent hole coded, ironically, by one of the other auditors. There were also two independent bugs, and the comments in the code for one of the bugs did not agree with the code. Either bug alone was harmless; together, combined with a common configuration mistake, they added up to a remote exploit. There was a plausible innocent explanation for why the comments and the code did not match. It remains unclear if this was a deliberate back door or a coincidence.

<sup>253</sup> Every software system has a date beyond which there will be no further patches. Microsoft, for example, lists its support plans at <http://windows.microsoft.com/en-us/windows/products/lifecycle>.

<sup>254</sup> For example, several vulnerabilities have been found that allow attacks against systems using the Secure Socket Layer (SSL) protocol, a widely used standard employed by many applications, including Web browsers, printers, and email clients, for encrypting Internet connections. See, e.g., Dan Goodin, *Hackers Break SSL Encryption used by Millions of Sites*, THE REGISTER (Sept. 19, 2011), [http://www.theregister.co.uk/2011/09/19/beast\\_exploits\\_paypal\\_ssl/](http://www.theregister.co.uk/2011/09/19/beast_exploits_paypal_ssl/).

<sup>255</sup> For example, all Internet Engineering Task Force (IETF) meetings and mailing lists are open to the public. See the IETF website at [www.ietf.org](http://www.ietf.org), and in particular *The Tao of IETF: A Novice's Guide to the Internet Engineering Task Force*, IETF § 4 (Nov. 2, 2012), <https://www.ietf.org/tao.html>.

¶172 Finally, there is the question of who in the government should be covered by guidelines mandating reporting. In this paper, we are concerned specifically with a law enforcement vulnerability lab. Should every U.S. government employee be included in the guidelines? Or only those developing law enforcement surveillance tools? The vast majority of government employees—even those who encounter security vulnerabilities—are not directly involved in developing wiretapping tools. For example, there are presumably system administrators in the Veterans Administration who occasionally discover security vulnerabilities in the course of their work. Should they become legally obligated to report? We propose that the reporting obligation be linked to the use of vulnerabilities for law enforcement purposes. An ordinary system administrator who discovers a vulnerability perhaps should report it, but the legal requirement should apply only to those who employ such vulnerabilities to conduct communications intercepts.

## VII. EXECUTIVE AND LEGISLATIVE ENFORCEMENT

¶173 When should reporting occur—at the time of discovery or purchase of the vulnerability, or at the time of working exploit? Should there be exceptions to the reporting rule in the case of an extremely important target, and how should that work? In this section, we attempt to answer these questions as well as discuss the role of oversight.

### A. *Enforcing Reporting*

¶174 We advocate that vulnerabilities law enforcement seeks to exploit be reported by default. There are a number of ways to implement and enforce such a policy.

¶175 The simplest way to implement a default reporting policy would be guidelines that mandate reporting under certain circumstances promulgated by the administration, likely the Department of Justice.<sup>256</sup> However, a guidelines-only approach has inherent weaknesses. First, the guidelines would be formulated, implemented, and enforced by the very department with the most interest in creating exceptions to the rule, and that most “pays the cost” when the tools it develops and uses are neutralized. Such conflicts of interest rarely end up with the strongest possible protections for the public.

¶176 Therefore, a legislative approach may be more appropriate. Perhaps as part of the appropriations bill that funds the exploit discovery effort, Congress could mandate that any vulnerabilities the unit discovers be reported; alternatively, a reporting mandate could be added to the wiretap statute. This second approach has the advantage that it is more permanent; however, amending the Wiretap Act has proven to be a long and contentious process. Regardless, and as noted above, such legislation would need to be carefully drafted to capture a range of different circumstances.

¶177 In the absence of a legislative fix, the best solution is for the judge authorizing the use of the vulnerability to insert a reporting requirement into the warrant or order. This provision could include a return date by which the requesting agency must certify that the vendor had received appropriate notification. Apart from providing an enforcement

---

<sup>256</sup> For example, the reporting requirement could be added to THE ATTORNEY GENERAL’S GUIDELINES FOR DOMESTIC FBI OPERATIONS (2008), available at <http://www.justice.gov/ag/readingroom/guidelines.pdf>.

mechanism, this approach allows for careful consideration of specific circumstances, including exceptional circumstances that might merit a delay.<sup>257</sup>

¶178 Finally, one might imagine that the legislature could create a tort cause of action for those harmed by a criminal exploitation of a vulnerability known to the government but not reported. This would perhaps be the most radical approach to ensuring government reporting, but it seems most unlikely. There is currently no obligation on anyone to report vulnerabilities; for Congress to suddenly create government liability for non-reporting seems improbable.<sup>258</sup> Our favored approach to ensure early government reporting of vulnerabilities discovered is thus a simple but unambiguous legislative mandate that the government report any zero-day vulnerabilities it seeks to exploit. We take no position here on financial liability or other remedies should it fail to do so.<sup>259</sup>

### B. *Exceptions to the Reporting Rule*

¶179 Although we have recommended that law enforcement report vulnerabilities upon discovery (or purchase), there may be exceptional cases when immediate reporting is not appropriate because immediate reporting of the vulnerability might lead to a target patching and preventing installation of a wiretap. In what circumstances should not reporting immediately be appropriate?

¶180 It is worth considering the principles employed in the closely related situation of emergency wiretaps. Title III includes an exception allowing wiretaps to be used without a warrant in emergency situations as long as a wiretap order is obtained within forty-eight hours.<sup>260</sup> The law states that an emergency situation exists when there is immediate danger of death or serious bodily injury, conspiratorial activities threatening national security, or conspiratorial activities characteristic of organized crime,<sup>261</sup> but practice is that warrantless wiretapping by law enforcement<sup>262</sup> is permitted only when there is an immediate threat to life such as kidnapping and hostage-taking situations.<sup>263</sup> Emergency

---

<sup>257</sup> Exceptional circumstances are discussed in the following subsection.

<sup>258</sup> Due in part to disclaimers in End User License Agreements (EULAs), there is in general no liability even for vendors or developers of insecure software. *See, e.g.*, Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425 (2008). However, the issue is a frequent topic of academic discussion and the situation could conceivably change. In some situations, a site operator can be held negligent. *See, e.g.*, *In re Heartland Payment Systems*, 851 F. Supp. 2d 1040, 1047–48 (S.D. Tex. 2012).

<sup>259</sup> We do not discuss or suggest remedies if the government fails to report vulnerabilities, as is urged in this paper. A radical legislative approach could be to permit damages for those harmed by the exploitation of a zero-day vulnerability that was known to the government but that the government had not reported. A more moderate approach could impose a reporting obligation on the government but disallow private recovery of damages if it fails to do so.

<sup>260</sup> 18 U.S.C. § 2518(7) (2006).

<sup>261</sup> *Id.*

<sup>262</sup> Note that we are discussing warrantless wiretaps for criminal investigations under Title III, not the legalities of the Bush administration's "terrorist surveillance" warrantless wiretapping program. *See, e.g.*, Barton Gellman, Dafna Linzer & Carol D. Leonnig, *Surveillance Net Yields Few Suspects*, WASH. POST, Feb. 5, 2006, <http://www.washingtonpost.com/wp-dyn/content/article/2006/02/04/AR2006020401373.html>.

<sup>263</sup> For a detailed discussion, see 9-7.112: *Emergency Interception*, U.S. ATT'YS MANUAL, [http://www.justice.gov/usao/eousa/foia\\_reading\\_room/usam/title9/7mcrm.htm#9-7.112](http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/7mcrm.htm#9-7.112) (last updated July 2012).

wiretapping is not done lightly, and requires approval of someone of no rank lower than an Associate Attorney General. Once the emergency wiretap is approved (approved, not installed) law enforcement has forty-eight hours to obtain a wiretap order.<sup>264</sup>

¶181 Assume a situation in which, using a wiretap warrant, law enforcement downloads software to the target's machine and finds that the target is running an unusual set of programs, e.g., using the OpenBSD operating system with the Lynx web browser.<sup>265</sup> Law enforcement lacks suitable tools for this particular setup. To exercise the actual wiretap, law enforcement must find a vulnerability and operationalize it. Experience (with, e.g., the iPhone jailbreak efforts<sup>266</sup>) suggests that in most cases, this will not take too long. If the vulnerability is immediately reported as soon as it is acquired, law enforcement runs the risk that the target's device may be patched before the operationalized exploit can be used.

¶182 As far as we know, the FBI has never reported any of the vulnerabilities used to plant CIPAV. There is thus apparently no legal requirement that currently requires law enforcement to report vulnerabilities, so we recommend a compromise. For public safety, the law should require that law enforcement report vulnerabilities to the vendor once they have been acquired or otherwise discovered, but there should also be an emergency exception similar to that of Title III. We recommend that in an emergency situation, law enforcement should have a forty-eight hour window past the usual reporting deadline in which to petition a court for a release from reporting the vulnerability until it has successfully installed a wiretap.

¶183 We expect that such a provision would rarely be invoked. First, most vulnerabilities will have been discovered and reported by law enforcement, and the tools that exploit them built and put in the arsenal for future use, well before there is any investigation that might use them. For such tools, there is no emergency—or even any investigation—to weigh against reporting at the time the vulnerability would be reported because any situations in which a vulnerability is used would come up long after the vulnerability has already been reported.

¶184 But there may be exceptional circumstances in which this pattern—vulnerabilities discovered and tools developed well in advance of their being used by law enforcement—is not followed. For example, we can imagine a very high-value organized crime investigation in which a target might be using a particular and well-hardened, non-standard platform for which no exploit tools are available in the “standard” arsenal. Law enforcement might devote targeted resources toward discovering vulnerabilities and developing tools for the specific devices used by the particular target. In such (likely very rare) situations, the investigation and target might be known at the time some vulnerability is discovered by law enforcement, and they might place a high priority on preserving their ability to exploit it during the case.

---

<sup>264</sup> 18 U.S.C. § 2518(7) (2006).

<sup>265</sup> OpenBSD is an open-source operating system based on Unix (available at <http://www.openbsd.org/>) and Lynx is a web browser (available at <http://lynx.isc.org/>). Because Lynx does not support graphics, it cannot have web bugs, embedded objects that track usage, making it particularly privacy protective. Both systems, which are relatively old by industry standards, continue to be developed, but neither has large market share.

<sup>266</sup> The best compendium of information on the history of iPhone jailbreaking is a Wikipedia page, *iOS Jailbreaking*, WIKIPEDIA, [https://en.wikipedia.org/w/index.php?title=IOS\\_jailbreaking&oldid=589152900](https://en.wikipedia.org/w/index.php?title=IOS_jailbreaking&oldid=589152900) (last modified Jan. 4, 2014).

¶185 The criteria for exemption must be as stringent as the Title III exemption. If emergency wiretaps are permitted only when there is imminent danger of death (e.g., a kidnapping or hostage-taking situation) then the situation for emergency use of a vulnerability without reporting must be equally dire.

¶186 Another issue with emergency use is that the vulnerability must be such that there is a low risk of serious harm resulting from its exploitation by others against innocent persons. As we have discussed, estimating such risk is quite difficult. Given the importance of preventing crime, the decision not to report must not be made lightly. The petition not to report must include not only an argument for the importance of the interception, but also an analysis of the harm that could be caused should the vulnerability be discovered and exploited by others during the period that law enforcement is operationalizing the tool. In weighing whether to delay reporting a vulnerability, the court should consider how likely it is that the vulnerability, having been discovered, can actually be exploited, and the damage that may result from such exploitation.

### C. *Providing Oversight*

¶187 There is potential danger that an operationalized exploit may proliferate past its intended target. Stuxnet<sup>267</sup> provides an interesting case in point. Although aimed at Iran, the malware spread to computers in other countries, including India and Indonesia.<sup>268</sup> It is unclear from the public record how this happened. It may have been due to a flaw in the code, as Sanger contends;<sup>269</sup> alternatively, it may have been foreseeable but unavoidable collateral damage from the means chosen to launch the attack against Iran. Either possibility, though, represents a process that may be acceptable for a military or intelligence operation but is unacceptable for law enforcement. Only the legally authorized target should be put at risk from the malware used.

¶188 Given the public policy issues raised by the use of vulnerabilities, it would be appropriate to have public accountability on the use of this technique. For example, annual reports on vulnerability use similar to the AO's Wiretap Reports, presenting such data as: How many vulnerabilities were used by law enforcement in a given year? Were they used by federal or state and local? Was the vulnerability subsequently patched by the vendor, and how quickly after being reported? Was the vulnerability used by anyone outside of law enforcement? Was the vulnerability exploited outside law enforcement during the period that law enforcement was aware of the problem but had not yet told the vendor? Did the operationalized vulnerability spread past its intended target? What damages occurred from its exploitation? Making such information open to public analysis should aid in decisions about the right balance between efficacy and public safety.<sup>270</sup>

---

<sup>267</sup> See *Stuxnet Dossier*, *supra* note 17.

<sup>268</sup> DAVID E. SANGER, *CONFRONT AND CONCEAL: OBAMA'S SECRET WARS AND SURPRISING USE OF AMERICAN POWER* 203–05 (2013).

<sup>269</sup> *Id.* Sanger's conclusion is somewhat controversial. See Steven Cherry, *Stuxnet: Leaks or Lies?*, IEEE SPECTRUM (Sept. 4, 2012), <http://spectrum.ieee.org/podcast/computing/embedded-systems/stuxnet-leaks-or-lies>.

<sup>270</sup> The same is true regarding data from the Administrative Office of the U.S. Courts' Wiretap Reports (available at [http://www.uscourts.gov/Statistics/WiretapReports/WiretapReports\\_Archive.aspx](http://www.uscourts.gov/Statistics/WiretapReports/WiretapReports_Archive.aspx)). For



*D. Regulating Vulnerabilities and Exploitation Tools*

¶189 As we have mentioned, even without considering its use by law enforcement, information about software vulnerabilities is inherently “dual use”—useful for both offense and defense. Related to the issue of reporting and proliferation is the question of how the law should treat information about vulnerabilities and the development of software tools that exploit them by non-law enforcement persons. Should information about vulnerabilities, and tools that exploit them, be restricted by law? How do existing statutes treat such information and tools?

¶190 The issue of how to handle such dual-use technologies is not new. The computer security community has grappled for years with the problem of discouraging illicit exploitation of newly discovered vulnerabilities by criminals while at the same time allowing legitimate users and researchers to learn about the latest threats, in part to develop effective defenses.<sup>271</sup> It is all but impossible to prevent information about vulnerabilities or software exploits that use them from getting in to the hands of criminals without hampering efforts at defense. On the one hand, information about zero-day vulnerabilities is coveted by criminals who seek unauthorized and illicit access to the computers of others. But the same zero-day information is also used, and sought out by, legitimate security researchers and computer scientists who are engaged in building defenses against attack and in analyzing the security of new and existing systems and software.

¶191 Even software tools that exploit vulnerabilities are inherently dual use. They can be used by criminals on the one hand, but are also useful to defenders and researchers. For example, computer and network system administrators routinely use tools that attempt to exploit vulnerabilities to test the security of their own systems and to verify that their defenses are effective. Researchers who discover new security vulnerabilities or attack methods often develop “proof of concept” attack software to test and demonstrate the methods they are studying. It is not unusual for software that demonstrates a new attack method to be published and otherwise made freely available by academics and other researchers. Such software is quite mainstream in the computer science research community.<sup>272</sup>

---

example, one of the authors of the present paper used Wiretap Report data to show that FBI claims about the importance of wiretaps to solve kidnappings was incorrect. Between 1969 and 1994 wiretaps were used in only two to three kidnappings a year (out of 450 kidnappings annually). DIFFIE & LANDAU, *supra* note 21, at 211.

<sup>271</sup> The question of the ethics of publishing vulnerability information far antedates computers. In 1857, Alfred Hobbs, in *Rudimentary Treatise on the Construction of Door Locks*, wrote, “A commercial, and in some respects a social, doubt has been started within the last year or two, whether or not it is right to discuss so openly the security or insecurity of locks. Many well-meaning persons suppose that the discussion respecting the means for baffling the supposed safety of locks offers a premium for dishonesty, by showing others how to be dishonest. This is a fallacy. Rogues are very keen in their profession, and already know much more than we can teach them respecting their several kinds of roguery.”

<sup>272</sup> Many security software packages that might appear to be criminal attack tools are actually designed for legitimate research and testing. For example, the *Metasploit* package (available at <http://metasploit.com>) is a regularly updated library of software that attempts to exploit known vulnerabilities in various operating systems and applications. Although it may appear at first glance to be aimed at criminals, it is actually intended for (and widely used by) system administrators and professional “penetration testers” to identify weaknesses that should be repaired in their systems.

¶192 The software used by malicious, criminal attackers to exploit vulnerabilities can thus be very difficult to meaningfully distinguish from mainstream, legitimate security research and testing tools. It is a matter of context and intent rather than attack capabilities *per se*, and current law appears to reflect this.

¶193 Current wiretap law does not generally regulate inherently dual-use technology. The provision of Title III concerned with wiretapping equipment, 18 USC § 2512, generally prohibits possession and trafficking in devices that are “primarily useful” for “surreptitious interception” of communications,<sup>273</sup> which does not appear to apply to a wide range of current software exploit tools developed and used by researchers. We believe this is as it should be. The security research community depends on the open availability of software tools that can test and analyze software vulnerabilities. Prohibiting such software generally would have a deleterious effect on progress in understanding how to build more secure systems, and on the ability for users to determine whether their systems are vulnerable to known attacks. In addition, we note that given that the majority of vulnerability markets are outside the U.S., and that national security agencies are heavy purchasers of these vulnerabilities,<sup>274</sup> regulating them is not a plausible option.

¶194 The specialized tools developed by law enforcement to collect and exfiltrate evidence from targets’ computers, however, might fall more comfortably under the scope of 18 U.S.C. § 2512 (2006) as it is currently written. These tools would not be developed to aid research or test systems, but rather to accomplish a law enforcement interception goal. They would have narrowly focused features designed to make their installation surreptitious and their ongoing operation difficult to detect. They would also have features designed to identify and collect specific data, and would have no alternative use outside the surreptitious interception application for which they were developed. Such tools, unlike those used by researchers, could more easily meet section 2512’s test of

---

<sup>273</sup> 18 USC § 2512(1) (2006) provides criminal penalties for any person not otherwise authorized who:

(a) sends through the mail, or sends or carries in interstate or foreign commerce, any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications;

(b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce; or

(c) places in any newspaper, magazine, handbill, or other publication or disseminates by electronic means any advertisement of—

(i) any electronic, mechanical, or other device knowing the content of the advertisement and knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications; or

(ii) any other electronic, mechanical, or other device, where such advertisement promotes the use of such device for the purpose of the surreptitious interception of wire, oral, or electronic communications, knowing the content of the advertisement and knowing or having reason to know that such advertisement will be sent through the mail or transported in interstate or foreign commerce . . . .

<sup>274</sup> Greenberg, *supra* note 186.

being “primarily useful” for “surreptitious interception,” and thus would be unlawful if someone “manufactures, assembles, possesses, or sells” them except under the circumstances spelled out in that section.

## VIII. CONCLUSION

¶195 Changes in telecommunications technologies led to the 1994 passage of CALEA. However, CALEA created problems because of software complexity and the fact that it introduces a security vulnerability. Due to further—and quite extraordinary—changes in the communications technologies since CALEA’s passage, the law enforcement wiretapping capabilities the law engendered are now in danger of failing; to prevent this, law enforcement now seeks to expand the CALEA regime to IP-based communications. As we have discussed, the changes in communications technologies since 1994 not only undermine the present version of CALEA, they make extending the CALEA model to modern communications systems highly problematic, creating serious security risks.

¶196 Nonetheless, there needs to be a way for law enforcement to execute authorized wiretaps. The solution is remarkably simple. Instead of introducing *new* vulnerabilities to communications networks and applications, law enforcement should use vulnerabilities already present in the target’s communications device to wiretap in the situations where wiretapping is difficult to achieve by other means.

¶197 The exploitation of existing vulnerabilities to accomplish legally authorized wiretapping creates uncomfortable issues. Yet we believe the *technique is preferable for conducting wiretaps against targets when compared to other possible methods of wiretapping, like deliberately building vulnerabilities into the network or device, would result in less security.*

¶198 We propose specific policies to limit the potential damage of using existing vulnerabilities. First, we recommend that in order to prevent rediscovery of the vulnerability and hence proliferation of the exploit, technical defenses should be implemented. Second, we recommend that, with rare exceptions, *law enforcement should report vulnerabilities on discovery or purchase.* This means our proposal may actually have the benefit of *increasing* security generally. Finally, because the exploit may allow far greater penetrations of the target device than would be permitted by a mere wiretap, we urge guidelines to ensure that law enforcement bar use of any other information found on the computer during the exploit (unless permitted by an additional warrant).

¶199 There is a critical difference in the societal dangers entailed in the use of targeted vulnerabilities compared with the installation of global wiretapping capabilities in the infrastructure. If abused, targeted vulnerability exploitation, like wiretapping in general, has the potential to do serious harm to those subjected to it. But it is significantly more difficult—more labor intensive, more expensive, and more logistically complex—to conduct targeted exploitation operations against all members of a large population. In other words, although vulnerability exploitation is very likely to be effective against any given target, it is difficult to abuse at large scale or in an automated fashion against *everyone*. Thus our solution provides better security than extending the model of CALEA to IP-based communications would.

¶200 Vulnerability exploitation has more than a whiff of dirty play about it; who wants law enforcement to be developing and using malware to break into users’ machines? We agree that this proposal is disturbing. But as long as wiretaps remain an authorized

investigatory tool, law enforcement will press for ways to accomplish electronic surveillance even in the face of communications technologies that make it very difficult. We are at a crossroads where the choices are to reduce everyone's security or to enable law enforcement to do its job through a method that appears questionable but that does not actually make us less secure. In this debate, our proposal provides a clear win for both innovation and security.

