2017

The 2016 Amendments to Criminal Rule 41: National Search Warrants to Seize Cyberspace, "Particularly" Speaking

Devin M. Adams
University of Richmond

Recommended Citation

Devin M. Adams, Comment, *The 2016 Amendments to Criminal Rule 41: National Search Warrants to Seize Cyberspace, "Particularly" Speaking*, 51 U Rich L. Rev. 727 (2017).

THE 2016 AMENDMENTS TO CRIMINAL RULE 41: NATIONAL SEARCH WARRANTS TO SEIZE CYBERSPACE, "PARTICULARLY" SPEAKING

INTRODUCTION

"One may know how to conquer without being able to do it."[1]

George Orwell's dystopia, with the ever-watchful Big Brother, has seemingly become a reality with the recently passed amendments to Rule 41 of the Federal Rules of Criminal Procedure.[2] Rule 41, governing searches and seizures, now permits magistrate judges to authorize agents—under a single warrant—to "remotely access," and simultaneously search, copy and seize information from an infinite number of unknown electronic devices in multiple districts anywhere in the country.[3] The unlimited jurisdiction provision is triggered when a device's location is obscured through "technological means," *or* if agents are investigating computer crimes in five or more districts[4]—regardless of whether the locations of the innumerable search targets are known. Absent clairvoyance, this begs the question of how Fourth Amendment warrant requirements are applied to such a sweeping search.

This comment examines this Fourth Amendment question through a close analysis of hacking technology and the government's technological response that has yet to appear before the United States Supreme Court. It concludes that the expanded jurisdiction of federal warrants under revised Rule 41 can function as a useful tool for combatting cybercrime and still satisfy the re-

[1] SUN TZU, THE ART OF WAR 35 (Lionel Giles trans., Global Grey 2013) (1910).

[2] GEORGE ORWELL, NINETEEN EIGHTY-FOUR 34 (Kindle ed., Planet eBook 2004) (1949) (describing a totalitarian state dictated by omnipresent government surveillance). This novel coined the term "Big Brother," which has come to be associated with secret surveillance. *Id.* at 3.

[3] *See* FED. R. CRIM. P. 41(b)(6); *id.* 41(b)(6)(A)–(B) advisory committee notes (2016).

[4] *See* FED. R. CRIM. P. 41(b)(6)(A)–(B) (referencing the Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5), which makes computer "hacking" a crime).

quirements of particularity and probable cause. However, to satisfy those constitutional requirements, magistrates must limit remote multi-computer searches to cases where it is likely that any targeted computer is participating in criminal activity. Magistrates will need to take particular care to limit searches that intrude on persons not involved in the unlawful activity that is the object of the search.

Part I provides a survey of encryption and anonymization technology universally employed by law-abiding citizens and criminals alike. Part II details how law enforcement has, and likely will, employ the techniques of computer hackers to circumvent these encryption technologies to conduct remote searches. Part III outlines a history of how the Rule 41 amendments were enacted. Part IV discusses the warrant for the largest hacking investigation and search in federal law enforcement history, Operation Pacifier. Included is an overview of federal court litigation that challenged the validity of the warrant, which may be appealed to the Supreme Court. Part V articulates and analyzes the "reasonable expectation" of privacy component in the Fourth Amendment as it relates to "remote access" searches. Part VI offers judges and defense counsel a constitutional framework of how to best assess probable cause and particularity in applications for remote access search warrants. Finally, Part VII concludes with an assessment and outlook on the use of remote searches and the need for judicial caution and attention to detail under the updated Rule 41.

I. UNDERSTANDING THE TECHNOLOGICAL TERMINOLOGY AND BACKGROUND

"If you know yourself but not the enemy, for every victory gained you will also suffer a defeat."[5]

Cyber security is currently a top priority for the United States, as we now face sophisticated cyber threats from state-sponsored hackers and organized cyber syndicates.[6] However, the FBI has

[5] TZU, *supra* note 1, at 34.

[6] *See Oversight of the Federal Bureau of Investigation: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. 3–5 (2016) (statement of James B. Comey, Director, Federal Bureau of Investigation), https://judiciary.house.gov/wp-content/uploads/2016/09/Director-Comey-Statement.pdf.

realized a growing gap in their pursuit of these cyber threats because these criminals are "Going Dark" and have become virtually invisible through the use of encryption based technology, which forms an administrative hindrance for agents seeking search warrants.[7] The amendments to Rule 41 are aimed at addressing these challenges, and apply in two circumstances: (1) where a suspect has hidden the location of their computer using technological means, or (2) where the crime involves criminals hacking computers located in five or more different judicial districts.[8] This brings a large population of computer users within law enforcement's reach as hacking crimes have become rampant in the news and hiding a computer through technological means encompasses a number of widely used anonymization technologies.

A. *The New Barrier for Law Enforcement —Criminals "Going Dark"*

The movement to change Rule 41 is the product of advancements in technology and changes in societal norms that have created the proverbial perfect storm. We now carry on our lives in the Internet of Things ("IoT").[9] At a limited cost, we now have the means to connect any device with an on and off switch to the Internet, including cell phones, coffee makers, washing machines, wearable devices, the jet engines of an airplane, or the drill of an oil rig.[10] Such a proliferation of technology connected to the ether opposes general notions of privacy, extends the reach of surveillance, and magnifies the potential for a breach of security. Criminals know this, and our increased reliance on technology has spawned a new generation of technically affluent criminals who have caused a rise in cybercrime.[11]

[7] *Id.*

[8] *See* FED. R. CRIM. P. 41(b)(6); Leslie R. Caldwell, *Rule 41 Changes Ensure a Judge May Consider Warrants for Certain Remote Searches*, U.S. DEP'T OF JUSTICE: JUSTICE BLOGS (June 20, 2016), https://www.justice.gov/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches.

[9] KAREN ROSE ET AL., THE INTERNET OF THINGS: AN OVERVIEW 3, 11 (2015), www.internetsociety.org/sites/default/files/ISOC-loT-overview-20151022.pdf (defining the term "Internet of Things" and noting that "[t]he Internet of Things is happening now . . . a revolutionary, fully connected 'smart' world").

[10] Jacob Morgan, *A Simple Explanation Of 'The Internet Of Things,'* FORBES (May 13, 2014, 12:05 AM), http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#33209d368284.

[11] S. SELECT COMM. ON INTELLIGENCE, S. REP. NO. 114-8, at 6 (2015).

This creates a challenge for federal agents who now face a modern criminal whose tools have evolved from a ski mask and firearm. Today's criminal uses computers and mobile devices to commit his crime. The black hats of today turn to cyber tools to target United States' interests and facilitate theft, extortion and other criminal activities.[12] The drug lords of today supply criminal enterprise with online storehouses hidden on the Dark Web, operating like eBay, which buy and sell narcotics, explosives, passports and pornography.[13] Rather than with brute force, vindictive nation-states gain and use cyber expertise to achieve strategic objectives and challenge perceived adversaries in cyberspace.[14] Legitimate companies supply a lucrative black market by developing and selling professional-quality invasion technologies, which makes for a well-equipped foreign and domestic threat campaign.[15]

These tech savvy criminals are further undeterred from participation because of the low cost of entry, perceived payoff, and lack of actual consequences.[16] The result is that the greatest threats of today no longer take on a militant form, and the modern munitions are the widely available free encryption technology, mobile-messaging applications, the dark web and virtual environments that bring to fruition criminal operations.[17] Furthermore, the scale and sophistication of the cybercriminal enterprise has become supreme, as criminals surreptitiously control armies of infected computers, known as botnets, to wage attacks and "conceal their identities and locations while perpetrating crimes ranging from drug dealing to online child sexual exploitation."[18]

[12] JAMES R. CLAPPER, STATEMENT FOR THE RECORD: WORLDWIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY 3–4 (2016), https://www.armed-services.senate.gov/imo/media/doc/Clapper_02-09-16.pdf.

[13] *See* Diana S. Dolliver, *How a Virtual 'Mob Boss' from Texas Became The New Face of Organized Crime*, THE CONVERSATION (July13, 2015, 6:21 AM), https://theconversation.com/how-a-virtual-mob-boss-from-texas-became-the-new-face-of-organized-crime-43685; *see also* United States v. Ulbricht, 31 F. Supp. 3d 540, 547 (S.D.N.Y. 2014).

[14] *See* S. SELECT COMM. ON INTELLIGENCE, S. REP. NO. 114-8, at 7–8.

[15] CLAPPER, *supra* note 12, at 3.

[16] *Id.* at 3.

[17] *Id.* at 6.

[18] *Cyber Crime: Modernizing Our Legal Framework for the Information Age: Hearing Before the S. Comm. on the Judiciary, Subcomm. on Crime and Terrorism*, 114th Cong. 9 (2015) (statement of David M. Bitkower, Deputy Assistant Attorney General, U.S. Dep't of Justice, Crim. Division), https://www.hsdl.org/?view&did=790581.

News of "hackers" and "hactivists" are now commonplace in the media.[19] Cyberattacks are responsible for disabling 1500 computers in the Pentagon,[20] claiming the private information of 83 million JP Morgan clients,[21] compromising the United States' electric grid,[22] manipulating the stock market,[23] penetrating the voter registry,[24] and holding hospital systems for ransom.[25]

The catalyst for the Rule 41 amendments is not the prominence of this cybercrime per se, but rather the second dilemma agents face—finding and investigating this branch of criminals. The FBI calls this problem "Going Dark."[26] Our modern criminal has "gone to school" to learn how to use encrypted security platforms built for gaming or other commercial purposes to evade detection and facilitate terrorism.[27] Specifically, the Going Dark problem has created a gap between agents' authority and the inherent ability to gather valuable evidence in cases ranging from organized

[19] *See* Tom Sorell, *Human Rights and Hactivism: The Cases of Wikileaks and Anonymous*, 7 J. HUM. RIGHTS PRAC. 391, 391–92 (2015), http://jhrp.oxfordjournals.org/content/7/3/391.full.pdf+html. "Hacktivists" engage in "hactivism:" "a form of political activism in which computer hacking skills are heavily employed against powerful commercial institutions and governments" to steal corporate secrets and reveal classified government information. *Id.*

[20] *Whacking Hackers*, NEWSWEEK (Oct. 9, 2007, 11:18 AM), http://www.newsweek.com/whacking-hackers-103531.

[21] Pete Brush, *Israeli Suspects in Giant JPMorgan Hack Deny Charges in NY*, LAW 360 (June 9, 2016, 7:03 PM), https://www.law360.com/articles/805660/israeli-suspects-in-giant-jpmorgan-hack-deny-charges-in-ny.

[22] Eric Beech, *Cyberspies Penetrate Electric Grid: Report*, REUTERS (Apr. 8, 2009, 9:22 AM), http://www.reuters.com/article/us-cyberattack-usa-idUSTRE53729120090408.

[23] Max Fisher, *Syrian Hackers Claim AP Hack That Tipped Stock Market by $136 Billion. Is it Terrorism?*, WASH. POST (Apr. 23, 2013), https://www.washingtonpost.com/news/worldviews/wp/2013/04/23/syrian-hackers-claim-ap-hack-that-tipped-stock-market-by-136-billion-is-it-terrorism/.

[24] Ellen Nakashima, *Russian Hackers Targeted Arizona Election System*, WASH. POST (Aug. 29, 2016), https://www.washingtonpost.com/world/national-security/fbi-is-investigating-foreign-hacks-of-state-election-systems/2016/08/29/6e758ff4-6e00-11e6-8365-b19e428a975e_story.

[25] Richard Winton, *Hollywood Hospital Pays $17,000 In Bitcoin To Hackers; FBI Investigating*, L.A. TIMES (Feb. 18, 2016, 10:44 AM), http://www.latimes.com/business/technology/la-me-ln-hollywood-hospital-bitcoin-20160217-story.html.

[26] *See generally 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) (statement of Valerie Caproni, General Counsel, Federal Bureau of Investigation) [hereinafter *Going Dark: Lawful Electronic Surveillance*].

[27] Margaret Coker et al., *How Islamic State Teaches Tech Savvy to Evade Detection*, WALL ST. J. (Nov. 16, 2015, 9:41 PM), http://www.wsj.com/articles/islamic-state-teaches-tech-savvy-1447720824.

crime and drug trafficking to terrorism and espionage.[28] Moreover, cybercrime transcends borders and has no territorial jurisdiction, whereas law enforcement and the judiciary must still play by the rules of the physical world.[29] Legislators, judges, United States attorneys, and the public must choose whether to prioritize privacy or security.[30]

Through agency rulemaking,[31] the Advisory Committee on Criminal Rules for the Judicial Conference of the United States made the decision to ease the burden on federal investigators and expand the jurisdictional scope of "remote access" search warrants for electronic devices.[32] With limited exceptions, prior to the amendments, judges generally could issue a warrant for a search only in their district.[33] However, with the jurisdictional limitations removed for remotely seeking electronically stored information, Rule 41 now provides few parameters for "remote access" searches. Consequently, the Fourth Amendment requirements are the last vestige for privacy protection before crossing the line into unmitigated general search warrants by law enforcement. In order to circumscribe electronic search warrants and apply the

[28] *See Going Dark: Lawful Electronic Surveillance*, *supra* note 26, at 10; *see also* Stephanie K. Pell, Jones*ing for a Privacy Mandate, Getting a Technology Fix—Doctrine to Follow*, 14 N.C. J.L. & TECH. 489, 522–25 (2013) (arguing that advancements in technology serve as a regulator alongside the courts and Congress to limit the Government's gaze, but the privacy-security-enhancing benefits of technology also prevent law enforcement from accessing communications content).

[29] *See* 28 U.S.C. § 636(a) (2012) (circumscribing magistrates judicial authority); H. MARSHALL JARRETT ET AL., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 84–85 (Office of Legal Educ., Executive Office for U.S. Attorneys ed., 3d ed. 2009) ("Agents should obtain multiple warrants if they have reason to believe that a network search will retrieve data stored in multiple locations.").

[30] *Deciphering the Debate Over Encryption: Industry and Law Enforcement Perspectives: Hearing Before the Subcomm. on Oversight and Investigation of the H. Comm. on Energy and Commerce*, 114th Cong. 2–3 (2016) (statement of Amy Hess, Executive Assistant Director, Federal Bureau of Investigation, Science and Technology Branch).

[31] *See generally* Rules Enabling Act, 28 U.S.C. §§ 2071–2074 (2012) (granting Article III courts general rulemaking authority).

[32] *Contra* Orin Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 805–06 (2004) (arguing that the legislative branch rather than the judiciary should create the primary investigative rules when technology is changing).

[33] *See* FED. R. CRIM. P. 41(b) (2)–(5) (authorizing out-of-district or extra-territorial warrants in cases where: (1) property in the district where the warrant is issued might be moved outside the district before the warrant is executed; (2) tracking devices, which may be monitored outside the district if installed within the district; (3) investigations of domestic or international terrorism; and (4) property located in a United States territory or a United States diplomatic or consular mission).

Fourth Amendment to a search of multiple unknown computers, it is important to fully understand which technology is involved and how a remote search is executed. Otherwise the private affairs of the innocent general populous could be inadvertently exposed to government agents. Given that warrants take place ex parte and rarely involve judicial opinions, this comment is intended to anticipate future case law by providing a "particular" framework and analysis for applying constitutional requirements to applications for, and challenges to, warrants under the new Rule 41(b)(6).

B. *"Concealed Through Technological Means"—Anonymity, Encryption, and the Dark Web*

The lexicon in this area can be foreign, but understanding the ways in which individuals remain anonymous and untraceable on the Internet is imperative. First, a new extraterritorial provision in Rule 41 is triggered if media or information "has been concealed through technological means."[34] Second, understanding the technology and its myriad of uses is important because this ultimately should play a role in determining whether a user of anonymization technology has a "reasonable expectation of privacy."[35]

Because of the way the Internet operates, internet service providers ("ISPs"), and in turn law enforcement, know our names, addresses, search histories, and internet protocol ("IP") address—which identifies the specific computer using the Internet.[36] With this much information exposed simply by logging onto the Internet, many people wish to surf the Web and exchange communications or sensitive information free from state or corporate surveillance.[37] Those who conceal their identity while online through anonymization technology are not just predators lurking in the corners of the Web, but also voters, whistle-blowers, authors of

[34] FED. R. CRIM. P. 41(b)(6)(A). For example, this would allow a judge in New York to issue a warrant for the search of a computer in California, executed by agents sitting at their desk in New York.

[35] *E.g.*, United States v. Jones, 565 U.S. 400, 400 (2012); Smith v. Maryland, 442 U.S. 735, 740 (1979) (citing a lineage of Fourth Amendment privacy cases); *see* Part V *infra*.

[36] *See* Eric Jardine, *The Dark Web Dilemma: Tor, Anonymity and Online Policing*, *in* GLOBAL COMMISSION ON INTERNET GOVERNANCE 2 (2015), https://www.cigionline.org/sites/default/files/no.21.pdf.

[37] *Id.*

controversial publications, journalists, investigators, and other government agents.[38] As noted, these benefits come with the drawback of creating a Dark Net—where most have never been—a place for illegal drugs, weapons, and child abuse imagery—where those engaged can deal without the risk of facing law enforcement or public scrutiny.[39] There are several readily available privacy enhancing technologies including proxy servers, virtual private networks ("VPNs"), encryption and anonymizing browsers like Tor.[40] Using any one of these on an electronic device would satisfy being "concealed through technological means."[41]

1. Proxy Servers

Widely utilized by governmental agencies, private companies and schools, a proxy server is simply a computer service that acts as an intermediary between senders and receivers of information.[42] If used correctly, the website you are visiting, and thus your ISP, will *only* be able to "see" the identifying information of the proxy service you are using.[43]

2. Virtual Private Networks

A VPN is a collection of devices that have the ability to both send and receive data among themselves.[44] Sensitive information can be passed among those within the network with an even

[38] Emin Caliskan et al., *Technical and Legal Overview of the Tor Anonymity Network*, NATO COOPERATIVE CYBER DEF. CTR. OF EXCELLENCE 24 (2015), https://ccdcoe.org/sites/default/files/multimedia/pdf/TOR_Anonymity_Network.pdf (illustrating that this also includes victims of abuse, witnesses to serious crimes, and intelligence officers).

[39] *See* Jardine, *supra* note 36, at 2–4.

[40] Ruogu Kang, Stephanie Brown, & Sara Kiesler, *Why Do People Seek Anonymity on the Internet? Informing Policy and Design*, SIGCHI CONF. ON HUMAN FACTORS IN COMPUTING SYS. 2657, 2661–62 (2013), https://www.researchgate.net/profile/Sara_Kiesler2/publication/262273589_Why_do_people_seek_anonymity_on_the_Internet_Informing_policy_and_design/links/561fb32b08aea35f267df808.pdf.

[41] *See* FED. R. CRIM. P. 41(b)(6)(A).

[42] Caliskan et al., *supra* note 38, at 4.

[43] *See* Foshoto Stephen Gbenga et al., *Development of An Identity Management System For a Web Proxy Server In a Tertiary Institution Using Anonymity Technology*, 11 INT'L J. PHYS. SCI. 157, 158 (2016), http://www.academicjournals.org/journal/IJPS/article-full-text-pdf/850997559614; Brad Chacos, *How (and Why) to Surf the Web in Secret*, PCWORLD (Nov. 7, 2012, 3:30 AM), http://www.pcworld.com/article/2013534/how-and-why-to-surf-the-web-in-secret.html.

[44] Paul Ferguson & Geoff Huston, *What Is a VPN?*, 1 INTERNET PROTOCOL J. 2, 2 (1998), http://www.cisco.com/c/dam/en_us/about/ac123/ac147/archived_issues/ipj_1-1/ipj_1-1.pdf.

greater degree of impunity because the information is also encrypted as it passes between each host of the subnetwork.[45] Hackers attempting to pry would only see the encrypted data.[46]

3. Tor, "The Onion Router"

The Dark Web, a term loosely used, is that part of the Internet accessible only through the onion router ("Tor").[47] As designed, circumventing Tor's obscuring capabilities requires significant time and advanced technical abilities,[48] which made the Tor service browser the bane of federal law enforcement until 2012.[49]

There are other similar service browsers. However, with an average of two million users per day in 2015, Tor is the predominate choice when seeking anonymity because the platform prevents covert observers from identifying which sites users are visiting, as well as the sites from identifying the visitor.[50] Tor's infrastructure is comprised of thousands of volunteer "relays" or "nodes" around the globe that traffic the information along a pathway.[51] Each node knows its predecessor and successor, but no other nodes in the path.[52] The information is heavily encrypted end to end along this broken path,[53] but is then unwrapped at each node (like the layers of an onion) and relayed downstream.[54] With regard to how much impunity Tor offers, tech scholars have analogized the Tor network to the postal service: one *cannot* see what

[45] *Id.* at 9.

[46] Caliskan et al., *supra* note 38, at 5.

[47] Tor is the brainchild of the United States Naval Research Laboratory ("NRL"), which made its debut in 1996 when three researches at NRL presented the project. *See generally* David M. Goldschlag, Michael G. Reed, & Paul F. Syverson, *Hidden Routing Information*, WORKSHOP ON INFO. HIDING (May 1996), https://www.onion-router.net/Publications/IH-1996.pdf.

[48] Caliskan et al., *supra* note 38, at 13.

[49] Kevin Poulsen, *The FBI Used the Web's Favorite Hacking Tool to Unmask Tor Users*, WIRED (Dec. 16, 2014, 7:00 AM), https://www.wired.com/2014/12/fbi-metasploit-tor/. The fact that Tor is free further incentivizes users. *See What Is Tor?*, TOR PROJECT: ANONYMITY ONLINE, https://www.torproject.org/.

[50] Gareth Owen & Nick Savage, *The Tor Dark Net*, GLOBAL COMM'N ON INTERNET GOVERNANCE 1 (Sept. 2015), https://www.cigionline.org/sites/default/files/no20_0.pdf.

[51] *Id.*

[52] Roger Dingledine et al., *Tor: The Second-Generation Onion Router*, 13th USENIX SECURITY SYMPOSIUM 1 (2004), http://www.nrl.navy.mil/itd/chacs/sites/www.nrl.navy.mil.itd.chacs/files/pdfs/Dingledine%20etal2004.pdf.

[53] Jardine, *supra* note 36, at 2.

[54] Dingledine et al., *supra* note 52, at 1 (explaining what has come to be known as "onion routing"); *see also* Caliskan et al., *supra* note 38, at 6–7.

happens in the sorting room, but can see how many letters every address posts and receives each day. Thus, encrypted data can only be observed leaving one person and arriving at the other and vice versa. [55]

Tor not only allows users to view content anonymously online, but individuals can also host anonymous content—a "dark" website—whereby the *site itself* moves around the Tor network in much the same way as described above.[56] With these hidden services individuals can feature political blogs and forums, or provide a marketplace for weapons and illegal drugs, or the distribution of child pornography.[57] However, Tor users are not automatically placed among questionable company. Should a Tor user wish to simply surf the Web anonymously without wading into the murky areas of the Internet, Tor may be used like Google Chrome or Mozilla Firefox to privately engage in routine activities.[58]

II. THE PREREQUISITES TO "HACKING," ITS FORMS AND RELATED TERMINOLOGY

"All warfare is based on deception. . . . Hold out baits to entice the enemy. Feign disorder, and crush him."[59]

Rarely does bank robbery today take place in person, and agents no longer need to break down a door to obtain evidence. Both are now effectuated via cyber expertise: computer hacking. A "hacker" is anyone "who surreptitiously uses or changes the information in another's computer system."[60] Hackers and law enforcement share a common challenge they must first overcome: entry. Gaining access to another's computer, requires "malware" or "malicious technology," which often comes in the form of software that is covertly deployed and can then be used to monitor or

[55] Owen & Savage, *supra* note 50, at 7.

[56] Jardine, *supra* note 36, at 2; Caliskan et al., *supra* note 38, at 11 (explaining that these sites have non-traditional URLs; the website addresses within Tor are algorithm generated characters followed by the suffix ".onion."); Dingledine et al., *supra* note 52, at 8.

[57] Owen & Savage, *supra* note 50, at 1. Large portions of this hidden part of the Internet is off Google's radar and creates a Dark Net for illicit activity. *See* Jardine, *supra* note 36, at 2.

[58] Jardine, *supra* note 36, at 2.

[59] TZU, *supra* note 1, at 26–27.

[60] *Hacker*, BLACK'S LAW DICTIONARY (10th ed. 2014).

gain control of another's computer system.[61] However, before the intruder can execute this malware, it must be delivered to the computer system.[62] This is accomplished by exploiting vulnerabilities: either a human weakness or a technical vulnerability in the target's system.[63] Hackers exploit a vulnerability and gain access to a computer in one of two primary methods: by employing social engineering or a "watering-hole" tactic. The means employed by those hackers in the news media, and the way in which agents have, and will, "remotely access" target computers pursuant to search warrants—are one and the same.

A. *Social Engineering: A Little Impersonation and Deception*

Social engineering exploits the flaws in human logic and our natural tendency to trust others or perform requested actions.[64] With this method, an intruder gains access to a target computer by first sending a repetitious pop-up ad or e-mail that masquerades as though it came from a legitimate and well-known business.[65] The ad or e-mail, unbeknownst to the target, is laced with malicious computer code that will be covertly deployed onto the target's computer merely by clicking on the ad or e-mail containing the intriguing subject line.[66] In computer parlance, this is the cyberworld's version of the "Trojan Horse."[67]

[61] *Malicious Technology*, BLACK'S LAW DICTIONARY (10th ed. 2014); *see also* Zango, Inc. v. Kaspersky Lab, Inc., 568 F. 3d 1169, 1171 (9th Cir. 2009) (describing "malware" and "malicious technology" and its effects).

[62] Thomas Rid & Ben Buchanan, *Attributing Cyber Attacks*, 38 J. STRATEGIC STUD. 4, 15 (2015), http://dx.doi.org/10.1080/01402390.2014.977382.

[63] *Id.* at 15–16; *see also* Steven M. Bellovin, Matt Blaze, Sandy Clark, & Susan Landau, *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1, 25–26 (2014) (detailing the panoply of ways to gain entry, including infected attachments in e-mail, malware on web pages, poor implementations of network protocols, and users downloading and voluntarily executing programs, believing that the program serves a desirable and credible purpose).

[64] Xin (Robert) Luo et al., *Social Engineering: The Neglected Human Factor for Information Security Management*, 24 INFO. RESOURCES MGMT. J. 1, 3 (2011), http://www.unm.edu/~xinluo/papers/IRMJ2011.pdf; *see also* SYMANTEC, INTERNET SECURITY THREAT REPORT 27–29 (Vol. 2016) [hereinafter INTERNET SECURITY THREAT REPORT], https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf (collecting examples of SE attacks).

[65] Luo et al., *supra* note 64, at 4.

[66] *See id.* at 3–4; Rid & Buchanan, *supra* note 62, at 16.

[67] The term gets its name from the Greek story of the Trojan War, where the Greeks offered the Trojans a peace offering in the form of a large wooden horse. *See Trojan Horse*, ENCYCLOPEDIA BRITANNICA (15th ed. 2002). However, Greek soldiers lay hidden inside, and once the Trojans wheeled the horse behind the gates and night fell, the Greek soldiers

1. The FBI Employs Social Engineering Tactics to Surreptitiously Gain Access

Pursuant to search warrants, federal agents have been deploying malware and spyware to conduct computer searches for nearly fifteen years, albeit in the primitive form of a keystroke logger.[68] By 2001, the FBI adapted their hacking capabilities and rebranded their malware as a Computer and Internet Protocol Address Verifier ("CIPAV"), which came to be known as the FBI's "Magic Lantern" for effectively searching unknown target computers.[69] For example, the FBI used social engineering via a fictitious e-mail from the Associated Press to identify the IP address of a terrorist sending bomb threats to administrators at Timberline High School in Lacey, Washington.[70]

Agents' covert method of deploying spyware was later cryptically renamed in its warrant applications as a request to deploy a Network Investigative Technique ("NIT"), an acronym still used today.[71] Such a warrant was approved to locate an anonymous culprit, identified only by the e-mail address texan.slayer@yahoo.com, who sent messages to county police in Colorado, pledging to

hidden inside the horse climbed out and let their confederates in to ravage the city of Troy. *Id.*

[68] *See, e.g.*, United States v. Scarfo, 180 F. Supp. 2d 572, 574 (D.N.J. 2001); *see also* Kevin Poulsen, *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats*, WIRED (July 18, 2007), http://archive.wired.com/politics/law/news/2007/07/fbi_spyware?currentPage=all (recounting the FBI's 1999 investigation of mobster Nicodemo Scarfo).

[69] *See* Ted Bridis, *FBI Is Building a 'Magic Lantern'*, WASH. POST (Nov. 23, 2001), https://www.washingtonpost.com/archive/politics/2001/11/23/fbi-is-building-a-magic-lantern/ca972123-83a8-46d8-b95c-c2edafda0fea/; Jennifer Lynch, *New FBI Documents Provide Details on Government's Surveillance Spyware*, ELECTRONIC FRONTIER FOUND.: DEEPLINKS BLOG (Apr. 29, 2011), https://www.eff.org/deeplinks/2011/04/new-fbi-documents-show-depth-government#footnote2_ab30fhg (providing links to documents).

[70] *See* Application and Affidavit for Search Warrant, *In re* 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, at 5–13 (W.D. Wash. June 12, 2007), http://www.politechbot.com/docs/fbi.cipav.sanders.affidavit.071607.pdf; *see also* Ellen Nakashima & Paul Farhi, *FBI Lured Suspect with Fake Web Page, But May Have Leveraged Media Credibility*, WASH. POST (Oct. 28, 2014), https://www.washingtonpost.com/world/national-security/fbi-lured-suspect-with-fake-web-page-but-may-have-leveraged-media-credibility/2014/10/28/e6a9ac94-5ed0-11e4-91f7-5d89b5e8c251_story.html. The teen in that case plead guilty and never challenged the warrant. *See* United States v. MySpace Account "Timberlinebombinfo," No. 3:07-mj-05114 (W.D. Wash. Jun 12, 2007).

[71] Third Amended Application for a Search Warrant, *In re* Matter of the Search of Network Investigative Technique ("NIT") for E-mail Address texan.slayer@yahoo.com, No. 1:12-sw-05685-KMT, at 1 (D. Col. Dec. 11, 2012) [hereinafter "NIT" Warrant for texan.slayer@yahoo.com], https://cryptome.org/2013/12/nit-email-search.pdf.

set off Ammonium Nitrate explosions if demands were not met.[72] In that case, agents used an e-mail tainted with malware to locate the unidentified source of the threats.[73] The warrant did not use the words "hack," "malware" or "spyware," but instead stated that "communications" would be sent "to cause an activating computer to send certain information to a computer controlled by the . . . FBI."[74] Although passively phrased, this is surreptitious entry via social engineering.

Absent prior familiarity, these warrants appear to request information that will simply be gleaned from the ether.[75] However, with an understanding of well-established methods of social engineering, and a cursory review of the pages of these warrant applications, one can see NIT means: surreptitiously installing software on a target's computer.

B. *Watering Hole Attacks or Drive-By-Downloads: Optimal for Searching the Masses*

A "watering hole" or "drive-by-download" tactic represents an insidious form of malware delivery in the black hat arsenal, whereby the mere connection to a website can result in the installation of malware on the user's computer. The malicious website silently passes malicious code to the victim, which then forces the browser to download, store, and silently execute a malicious application.[76] This method of delivery involves a remote injection of

[72] *See id.* at 4–15; *see also* Craig Timberg & Ellen Nakashima, *FBI's Search for 'Mo,' Suspect In Bomb Threats, Highlights Use of Malware For Surveillance*, WASH. POST (Dec. 6, 2013), https://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html?utm_term+.7dfb14dff7c2.

[73] *See* "NIT" Warrant for texan.slayer@yahoo.com, *supra* note 71, at 1, 5.

[74] *Id.* at 5, 16; *see also* Timberg & Nakashima, *supra* note 72 (resulting NIT search returned an IP address from Tehran, Iran). For another example of an NIT warrant used to apprehend an evasive suspect in a bank fraud and identity theft scheme, see Affidavit of Justin E. Noble in Support of Application for Search Warrant, *In re* Search of Network Investigative Technique ("NIT") for E-mail Address 512socialeedia@gmail.com, No. 12-mj-748-ML, at 5, 12 (W.D. Tex. Dec. 18, 2012) [hereinafter "NIT" Warrant for E-mail Address 512socialmedia@gmail.com], http://ia800205.us.archive.org/23/items/gov.uscourts.txwd.597669/gov.uscourts.txwd.597669.1.1.pdf.

[75] *See, e.g.*, "NIT" Warrant for E-mail Address 512socialmedia@gmail.com, *supra* note 74, at 12; *see also* Brian L. Owsley, *Beware of Government Agents Bearing Trojan Horses*, 48 AKRON L. REV. 315, 324–337 (2015) (discussing in detail the facts of the social engineering cases mentioned in this comment).

[76] Long Lu et al., *BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections*, 17TH ACM CONF. ON COMPUTER COMM. SECURITY 440, 440 (2010), http://dl.acm.org/ft_gateway.cfm?id=1866356&ftid=849819&dwn=1&CFID=850839721&C

malicious code into a website, which will then search a target computer when passed onto visiting internet users.[77] For obvious reasons hackers opt for this method of delivery because it provides a larger platform for delivery, and in turn, a greater number of computers will be accessed by the intruder.[78]

1. Instances of Federal Agents Taking Advantage of "Watering Hole" Tactics

At first glance, it is difficult to tell whether agents will use social engineering or a watering hole method in an NIT warrant application because they both use the term NIT to denote how the search will be executed.[79] The giveaway is in the title of the warrant: one is for a specific e-mail account[80] and the other is for *all computers* accessing a website.[81] Deciphering how a watering hole "search" will be executed is further complicated by the fact that the description of the NIT in a warrant application is couched in the pacifying terms that the website will be augmented "with some additional computer instructions . . . designed to cause the 'activating' computer to deliver certain information to . . . the government."[82] This evasive terminology simply means code is surreptitiously pushed onto all visitors of a website, which then

FTOKEN=25126908; *see also* Marco Cova et al., *Detection and Analysis of Drive-by-Download Attacks and Malicious JavaScript Code*, 19TH INT'L CONF. ON WORLD WIDE WEB 281, 281 (2010), https://cs.UCSb.edu/~virginia/publications.2010_cova_Kniegel_vigna_wepawet.pdf.

[77] *See* Rid & Buchanan, *supra* note 62, at 16 (clarifying that no user action is required and no symptoms of the infection may ever manifest); Lu et al., *supra* note 76, at 441.

[78] *See* INTERNET SECURITY THREAT REPORT, *supra* note 64, at 38.

[79] *Compare* Application for a Search Warrant, *In re* Search of Computers that Access the Website "Bulletin Board A", No. 8:12-MJ-356, at 31 (D. Neb. Nov. 16, 2012) [hereinafter Warrant for Computers that Access the Website "Bulletin Board A"], https://www.documentcloud.org/documents/1261620torpedo-affidavit.html (utilizing watering hole deployment), *with* "NIT" Warrant for texan.slayer@yahoo.com, *supra* note 71, at 20 (utilizing socially engineered e-mail).

[80] *See, e.g.*, "NIT" Warrant for texan.slayer@yahoo.com, *supra* note 71, at 1.

[81] *See, e.g.*, Warrant for Computers that Access the Website "Bulletin Board A," *supra* note 79, at 1.

[82] *Id.* at 30. Cryptic explanations of technology are not unusual for federal agents. *See* Stephanie K. Pell & Christopher Soghoian, *A Lot More Than a Pen Register, and Less Than a Wiretap: What the Stingray Teaches Us About How Congress Should Approach the Reform of Law Enforcement Surveillance Authorities*, 16 YALE J. L. & TECH. 134, 161–63 (2013) (discussing the government's lack of candor to judges when seeking authority to use "StingRay" cell phone tracking devices, and quoting Judge Owlsey stating, "I may have seen them before and not realized what it was, because what they do is present an application that looks essentially like a pen register application").

commands the users' computers to send information to federal agents.[83]

By way of illustration, pursuant to an NIT warrant in Operation Torpedo, agents apprehended a child pornography enterprise operated through a hidden website on the Tor browser.[84] The warrant authorized inserting code onto an illicit website that would then result in the search of any computer "wherever located," that accessed the images section of the website or viewed a private message.[85] With the information obtained from the search, agents were able to prosecute over a dozen visitors to the site.[86]

The largest watering hole search campaign in federal law enforcement history, occurred recently and is discussed in depth in Part IV. While there are other suspected examples of agents turning websites into watering holes in order to apprehend those hiding behind Tor,[87] motions to unseal those warrants are pending.[88]

C. *The Final Component in a Successful Hacking Campaign: A Zero-Day Vulnerability*

Zero-day vulnerabilities are pivotal to gaining entry into any electronic device. A zero-day vulnerability is an "unknown flaw in a computer program that exposes the program to external manipulation," and can be exploited from the "zero-th" day of discov-

[83] *Compare* Lu et al., *supra* note 76, at 441 ("[A]ll drive-by exploits begin with a remote code injection . . . within the browser . . . . [T]he shellcode effectively coerces the now tainted browser into fetching a remote malware application . . . and executing it on the victim's host.), *with* Warrant for Computers that Access the Website "Bulletin Board A," *supra* note 79, at 30, 32.

[84] *See* Warrant for Computers that Access the Website "Bulletin Board A," *supra* note 79, at 32, 34; Kevin Poulsen, *Visit the Wrong Website, and the FBI Could End Up in Your Computer*, WIRED (Aug. 5, 2014, 6:30 AM), https://www.wired.com/2014/08/operation_torpedo/ (detailing the facts of Operation Torpedo).

[85] Warrant for Computers that Access the Website "Bulletin Board A," *supra* note 79, at 31–32, 35. The information obtained included the IP address, unique session identifier, and the type of operating system running on the computer. *Id.* at 35.

[86] Poulsen, *supra* note 84. Litigation from defendants contesting the warrant was limited but ultimately unsuccessful. *See* United States v. Pierce, No. 8:13CR106, 2014 U.S. Dist. LEXIS 147114, at *18 (D. Neb. Oct. 14, 2014) (denying a collection of suppression motions from multiple defendants).

[87] *See, e.g.*, Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, WIRED (Sept. 13, 2013, 4:17 PM), http://www.wired.com/2013/09/freedom-hosting-fbi.

[88] *See* Motion to Unseal Court Docket Sheet, *In re* Sealed Docket Sheet Associated with Malware Warrant Issued on July 22, 2013, No. 1:16-CV-03029 (D. Md. Aug. 29, 2016).

ering the vulnerability.[89] A zero-day vulnerability is simply knowledge that there is a flaw in an operating system, and the zero-day exploit is then the malware code designed to take advantage of that vulnerability.[90] The code will be attached to an e-mail or embedded in the website, passed onto the target, and allow the intruder to gain control over the target's computer system.[91]

Because the essential vulnerabilities are discovered and not made, there is a black market for both the knowledge of the vulnerability, and the code that has already been designed to exploit the known vulnerability.[92] In order to carry out NIT searches, the government is a participant in the black market for zero-day vulnerabilities.[93] This involvement raises the concern of whether the government should be reporting knowledge of these vulnerabilities to software developers, like Microsoft, or keeping them in reserve to execute the next cyber-warrant in an NIT. With the jurisdictional limitations lifted on granting NIT warrants under Rule 41, agents will likely seek to use such warrants more often, and therefore the government will have an increased need for zero-day vulnerabilities.

D. *Botnets, and "Damaged" Within the Meaning of Rule 41(b)(6)(B)*

The second added extraterritorial provision in Rule 41 is triggered if the investigation involves computer crimes[94] "where the

[89] Mailyn Fidler, *Regulating the Zero-Day Vulnerability Trade: A Preliminary Analysis*, 11 J.L. & POL'Y FOR THE INFO. SOC'Y 405, 408 (2015). There is no perfect system, and zero-day vulnerabilities exist in Microsoft, Internet Explorer, Adobe, Apple products, and even our most secure digital infrastructure. *Id.*; INTERNET SECURITY THREAT REPORT, *supra* note 64, at 39 (reporting that on average a new zero-day vulnerability was discovered every week in 2015).

[90] Fidler, *supra* note 89, at 408–09.

[91] *See* Ben Buchanan, *The Life Cycles of Cyber Threats*, 58 SURVIVAL: GLOBAL POL'Y & STRATEGY 39, 40, 42 (2016), https://www.iiss.org/-/media//silos/survival/2016/survival/58-1-03-buchanan/58-1-03-buchanan.pdf (outlining that discovery and development of the exploit occur before introduction).

[92] *See* Bellovin, Blaze, Clark, & Landau, *supra* note 63, at 42; Fidler, *supra* note 89, at 410; INTERNET SECURITY THREAT REPORT, *supra* note 64, at 38.

[93] *See* Bellovin, Blaze, Clark, & Landau, *supra* note 63, at 41–42, 47; Fidler, *supra* note 89, at 411–12. Both articles focus heavily on zero-day exploits and the government's involvement in the market, as well as provide well-articulated policy concerns. Although Bellovin, Blaze, Clark, and Landau focus on the vulnerabilities used to execute wiretaps, the same principles and concerns apply in the computer context.

[94] *See* 18 U.S.C. § 1030(a)(5) (2012) (indicating that it is a criminal violation to know-

media are protected computers that have been damaged."[95] "Damaged," as used in Rule 41, means any impairment to the integrity of a program or system.[96] If a computer user has been the victim of a social engineering or watering hole attack, or unsuspectingly caught in a botnet, the user's computer would fall within the definition of "damaged" and thus be exposed to the extraterritorial search operations of federal agents.[97]

A botnet, referenced in the Rule 41 advisory committee notes,[98] is a group of computers that have been infected with malicious software, whereby millions of computers become part of a "zombie army" subject to the control of the "botmaster."[99] When this occurs computer owners are unaware, unable to resist, and can be made to perform automated tasks over the Internet without knowing it.[100] Unwittingly, users may be helping criminals.[101] The reality of the IoT is that it allows criminals to create unprecedented armies of botnets, which can be used or sold for a relatively inexpensive price.[102] Relatedly and even more unsettling, is that a large portion of the population is susceptible to a search for unwitting involvement in a botnet under the new Rule 41(b)(6)(B).

ingly transmit a program or code and access a protected computer without authorization).

[95] FED. R. CRIM. P. 41(b)(6)(B).

[96] *See* 18 U.S.C. § 1030(e)(8) (2012); FED. R. CRIM. P. 41(b)(6) advisory committee's note to 2016 amendments (giving "damage" the meaning provided in 18 U.S.C. § 1030(e)(8)).

[97] *See* 18 U.S.C. § 1030(e)(8); *see also supra* Part II.A–B (discussing the mechanics of social engineering and watering hole attacks). This is concerning because 8 percent of global botnet activity originates in the United States, and malware is linked to 1 in 3172 websites, as well as 1 in 220 e-mails. *See* INTERNET SECURITY THREAT REPORT, *supra* note 64, at 8–9, 60.

[98] FED. R. CRIM. P. 41(b)(6)(B) advisory committee's notes to 2016 amendments.

[99] Kalpna Midha et al., *An Introduction to Botnet Attacks and It's Solutions*, 1 INT'L J. COMPUTER APPLICATIONS & INFO. TECH. 37, 37 (2012), http://www.ijcait.com/IJCAIT/128R.pdf; *Botnets 101: What They Are and How to Avoid Them*, FBI: UCR (June 5, 2013), https://ucr.fbi.gov/news/news_blog/botnets-101/botnets-101-what-they-are-and-how-to-avoid-them (noting that infected computers in a botnet can number in the millions).

[100] Midha et al., *supra* note 99, at 37; David J. Malan, Rapid Detection of Botnets through Collaborative Networks of Peers 1 (June 7, 2007) (unpublished Ph.D. thesis, Harvard University), http://nrs.harvard.edu/urn-3:HUL.InstRepos:2961233.

[101] Midha et al., *supra* note 99, at 37. Typically, the botmaster uses his drone army to facilitate a distributed denial of service attack ("DdoS"), in which the drone army initiates a flood of data requests directed at the target system, which shuts down due to the overwhelming amount of requests. *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 443–45 (2012) (noting that DDoS attacks can be used against hospitals and defense systems).

[102] INTERNET SECURITY THREAT REPORT, *supra* note 64, at 8–9, 57, 60, 66 (noting the size and scope of attacks and the readily available opportunity to order a DDoS for $10 to $1000 per day).

III. THE PROPOSAL AND THE PROCESS TO AMEND FEDERAL RULE 41

"[T]he soldier works out his victory in relation to the foe whom he is facing . . . so in warfare there are no constant conditions."[103]

In early 2013, agents in Texas requested a warrant to remotely install data extraction software on a target computer—location and suspect unknown.[104] Once installed, the software had the capacity to search the computer's hard drive, activate the computer's built-in camera, generate latitude and longitude coordinates for the computer's location, and transmit the extracted data to FBI agents.[105] The court was unaware of a reported case which discussed the government's proposed technique within the context of a Rule 41 search, and expressed concern that the application contained little to no explanation of how the target computer would be found.[106] The court rejected the government's request.[107] Still the court remarked, "there may well be a good reason to update the territorial limits of [Rule 41] in light of advancing computer search technology."[108] Because of this decision, and others like it, five months later the Department of Justice set the gears in motion to change Rule 41.[109]

A. *The Proposal to Amend Rule 41*

The Department of Justice ("DOJ") presented to the Advisory Committee on Criminal Rules a proposal to remove the obstruction impairing the ability of law enforcement to investigate multi-

[103] TZU, *supra* note 1, at 46.

[104] *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 755 (S.D. Tex. 2013).

[105] *Id.*

[106] *Id.* at 758–59 n.10. The court also expressed concerns about collateral damage. *Id.* at 759.

[107] *Id.* at 758–61 (holding that the warrant application failed to satisfy the Fourth Amendment's particularity requirement and standards for video surveillance, and also violated Rule 41 jurisdictional limitations).

[108] *Id.* at 761.

[109] Letter from Mythili Raman, Acting Assistant Attorney Gen., to the Hon. Reena Raggi, Chair, Advisory Comm. on the Criminal Rules (Sept. 18, 2013), *in* Advisory Comm. on Criminal Rules, Materials for April 7–8, 2014 [hereinafter Advisory Comm. Materials for April 7–8], http://www.uscourts.gov/sites'default/files/fr_import/CR2013-10.pdf (citing *In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753 (S.D. Tex. 2013), and the court's recommendation to update the territorial limits of Rule 41).

district internet crimes. The proposed Rule 41 change specifically addressed limitations faced by law enforcement in two situations: "(1) where the warrant sufficiently describes the computer to be searched but the district within which a computer is located is unknown, and (2) where the investigation requires law enforcement to coordinate searches of numerous computers in numerous districts."[110] The DOJ avowed that updating Rule 41 in this regard would allow law enforcement to prosecute the increasing number of criminals who use anonymization technologies, as well as pursue the sophisticated botnet attacks launched from multiple computers in multiple districts.[111] The DOJ supported the proposal with three sample warrants to show how agents might apply for authorization to execute an NIT search warrant.[112] As discussions progressed the advisory committee made clear that "the proposed amendment's language speaks directly only to venue, and . . . the government must satisfy constitutional requirements with respect to any warrant."[113]

At the subcommittee phase, an enthusiastic debate began with concerns that Rule 41 should address the first of the DOJ's challenges, but should not allow multiple searches in multiple districts.[114] Specifically, some were concerned that in the context of searching digitally stored information, the proposed change would obviate the prevailing practice of knock, seize, and search offsite, as well as incentivize agents to circumvent the practice of

[110] *See* Advisory Comm. Materials for April 7–8, *supra* note 109, at 171. The amendments also allow delayed notice of the search, however, this was already a part of Rule 41, and seeking delayed notice in these circumstances is not a departure from the norm. *See* 18 U.S.C. 1302 (2012); FED. R. CRIM. P. 41(f)(3). For this reason, this comment does not focus on this aspect of the amendments.

[111] *See* Advisory Comm. Materials for April 7–8, *supra* note 109, at 172–73 (contending that seeking ninety-four warrants in ninety-four districts is impractical).

[112] Memorandum from Jonathan J. Wroblewski, Dir., Office of Pol'y and Leg. to Judge John F. Keenan, Chair, Subcomm. on Rule 41 (Jan. 17, 2014), *in* Advisory Comm. Materials for April 7–8, *supra* note 109, at 179–235 (providing examples of a warrant for an investigation of a series of bomb threats, a warrant for a child pornography website operating as a "hidden service" on the Tor network, and a warrant that would be sought in a botnet investigation).

[113] Advisory Comm. Materials for April 7–8, *supra* note 109, at 155.

[114] *Compare* Memorandum from Orin Kerr to Members of the Rule 41 Subcomm. (Feb. 3, 2014), *in* Advisory Comm. Materials for April 7–8, *supra* note 109, at 239–41 (raising concerns over forum shopping, and the criticism that a search of multiple locations not owned by the same person violates the particularity requirement), *with* Memorandum from Jonathan J. Wroblewski, Dir., Office of Pol'y and Legis. to Judge John F. Keenan, Chair, Subcomm. on Rule 41 (Feb. 7, 2014), *in* Advisory Comm. Materials for April 7–8, *supra* note 109, at 246–47 (addressing concerns raised by Professor Orin Kerr).

working with ISPs before obtaining evidence.[115] After airing these issues, the subcommittee made stylistic changes and in early March 2014 concluded that there were compelling justifications to advance the proposal and seek public comment.[116] The advisory committee then met in early April 2014 and recommended the Rule 41 proposal for public comment,[117] and stated in the report that "the use of anonymizing software to mask the location of a computer should not prevent the issuance of a warrant."[118] In August 2014, the public comment period was opened for the proposed Rule 41 amendments.[119]

B. *Notice and Comment Period—Opponents and Supporters*

Leading technology companies like Google, as well as, prominent civil rights groups, such as the American Civil Liberties Union, presented a gamut of concerns and made a compelling case against the Rule 41 changes.[120] Opponents portrayed the proposal

[115] *See* Memorandum from Orin Kerr to Members of the Rule 41 Subcomm. (Feb. 8, 2014), *in* Advisory Comm. Materials for April 7–8, *supra* note 109, at 251–52 (citing Electronic Communications Privacy Act (ECPA), 18 U.S.C. § 2703 (2012)). *But see* Memorandum from Jonathan J. Wroblewski, Dir., Office of Pol'y and Leg. to Judge John F. Keenan, Chair, Subcomm. on Rule 41 (March 5, 2014), *in* Advisory Comm. Materials for April 7–8, *supra* note 109, at 262–63 (addressing the particularity requirement for remote access searches on a "tracking device" rationale, and alternatively that jurisprudence permits a search of more than one piece of property).

[116] Memorandum from Sara Beale and Nancy King, Reporters to Members, Criminal Rules Advisory Comm. (Mar. 17, 2014), *in* Advisory Comm. Materials for April 7–8, *supra* note 109, at 155–61.

[117] Draft Minutes of Advisory Comm. on Criminal Rules (Apr. 7–8, 2014), *in* Comm. on Rules of Practice and Procedure. Materials for May 29–30, 2014 Meeting 532–33 [hereinafter Advisory Comm. Materials for May 29–30], http://www.uscourts.gov/sites/default/files/fr_import/ST2014-05.pdf.

[118] Memorandum from the Hon. Reena Raggi, Chair, Advisory Comm. on Criminal Rules to the Hon. Jeffrey S. Sutton, Chair, Comm. on Rules of Practice and Procedure (May 5, 2014), *in* Advisory Comm. Materials for May 29–30, *supra* note 117, at 485–86.

[119] *See* Memorandum from the Hon. Reena Raggi, Chair, Advisory Comm. on Criminal. Rules to the Hon. Jeffrey S. Sutton, Chair, Comm. on Rules of Practice and Proc. (May 5, 2014, revised July 2014), *in* Preliminary Draft of Proposed Amendments to the Fed. Rules of App., Bankr., Civ., and Crim. Proc. 3, 319, 325, 327 [hereinafter Prelim. Draft & Request for Comment], https://www.regulations.gov/contentStreamer?documentId=USC-RULES-CR-2014-0004-0001&disposition=attachment&contentType=pdf (labeling "remote access searches" as sending surveillance software over the internet).

[120] *See generally* Richard Salgado, Google Inc., Comment Letter on Proposed Amendment to Fed. R. Crim. P. 41 (Feb. 13, 2015) [hereinafter Salgado, Comment Letter], https://www.regulations.gov/contentStreamer?documentId=USC-RULES-CR-2014-0004-0029&attachmentNumber=1&disposition=attachment&contentType=pdf (writing in opposition to the proposed changes to Rule 41); ACLU, Second ACLU Comment Letter on Proposed Amendment to Rule 41 Concerning "Remote Access" Searches of Electronic Storage Media (Oct. 31, 2014) [hereinafter Second ACLU Comment Letter], https://www.regulations.

as a substantive expansion on the government's investigative authority, which raised a number of emphatic constitutional, legal, and geopolitical concerns.[121] A theme among those in opposition was that such sweeping changes involving individual privacy, as in the past, ought to be the work of congressional lawmaking.[122] In that same vein, objectors urged that any accommodation for the administrative burdens on law enforcement should reflect a statutory regime similar to the Wiretap Act,[123] and entail a prior determination that the target computer is not used for newsgathering before issuing a remote access warrant.[124]

Given the global nature of the Internet, and because by definition the target of the search is *unknown*, naturally concerns were also raised that a search outside of the United States could be implicated, thereby encroaching on foreign relations.[125] In addition, commenters requested answers on how Fourth Amendment requirements could be met for an untold number of unknown suspects.[126] Still others warned of potential forum shopping for

gov/contentStreamer?documentId=USC-RULES-CR-2014-0004-0013&attachmentNumber=1&disposition=attachment&contentType=pdf (explaining concerns with the proposed amendments to Rule 41).

[121] *E.g.*, Salgado, Comment Letter, *supra* note 120, at 1.

[122] *See, e.g.*, *id.* at 5–6 (referencing the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1804 (2012); Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2518; Stored Communications Act, 18 U.S.C. §§ 2701; Pen Registers and Trap and Trace Act, 18 U.S.C. § 3123; and USA PATRIOT Act, 50 U.S.C. § 1842).

[123] *See, e.g.*, Nat'l Ass'n of Criminal Defense Lawyers, Comment Letter on Proposed Amendments to Rule 41 of the Fed. R. Crim. P., at 2–3, 5 (Feb. 17, 2015) [hereinafter NACDL Comment Letter], https://www.regulations.gov/contentStreamer?documentId=USC-RULES-CR-2014-0004-0038&attachmentNumber=1&disposition=attachment&contentType=pdf (specifically arguing that network searches should be limited to a subset of serious offenses, rather than permitted in all cases); *see also* Salgado, Comment Letter, *supra* note 120, at 9 (suggesting that as with Title III warrant requirements under the Wiretap Act, 18 U.S.C. § 2518, agents should be required to satisfy mandates, such as exhausting other investigative techniques).

[124] *See* Reporters Comm. for Freedom of the Press, Comment Letter on the Proposed Amendment to Fed. R. Crim. P. 41 Concerning Remote Access Searches of Electronic Storage Media and Electronic Information, at 1–4 (Feb. 17, 2015), https://www.regulations.gov/contentStreamer?documentId=USC-RULES-CR-2014-0004-0047&attachmentNumber=1&=1&disposition=attachment&contentType=pdf. With limited exceptions, failure to make such a determination contravenes the Privacy Protection Act of 1980, 42 U.S.C. § 2000aa(a), passed in response to *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978).

[125] *See, e.g.*, Center for Democracy & Technology, Written Statement Before the Judicial Conference Advisory Comm. on Criminal Rules, at 3–4 (Oct. 24, 2014), https://www.regulations.gov/contentStreamer?documentId=USC-RULES-CR-2014-0004-0009&attachmentNumber=1&disposition=attachment&contentType=pdf (noting that such searches, although not within the Fourth Amendment, are typically addressed under the Mutual Legal Assistance Treaty process).

[126] *See, e.g.*, Second ACLU Comment Letter, *supra* note 120, at 21–22.

the most pliant or technologically naïve judges,[127] and most repeatedly, critics forecasted collateral damage and disapproved of agents executing remote searches by foisting malware onto numerous systems and compromising computer integrity.[128]

The DOJ countered and was joined by other national councils and associations who believed the rule changes were necessary.[129] The constitutionality of the proposal was defended with remarks that the purpose of the search is merely to discover the place to be searched,[130] and assurances were extended that the proposed changes would merely ensure that some court is available to *consider* whether a warrant application comports with the Fourth Amendment.[131] In conclusion, DOJ representatives denied any abrogation of the Wiretap Act,[132] averred that Rule 41 remains in continuity with the Privacy Protection Act,[133] and clarified that the use of remote searches is "not new."[134]

The public comment chapter concluded with a public hearing on November 5, 2014,[135] followed by advisory committee approval in March 2015,[136] and unanimous Standing Committee approval

[127] *See, e.g.*, NACDL Comment Letter, *supra* note 123, at 4–5.

[128] *See, e.g.*, *id.* at 5. *See generally* 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) (outlining primary technology and policy concerns surrounding the amendments up to the time they were submitted to the U.S. Supreme Court).

[129] *See, e.g.*, Robert J. Arello, President, Federal Bar Council, Comment Letter on Proposed Amendments to Fed. R. Crim. P. 4 and 41, at 7 (Oct. 27, 2014) (concluding the courts will answer these questions "in due course").

[130] David Bitkower, Deputy Assistant Attorney Gen., Response to Comments Concerning Proposed Amendment to Rule 41, at 4 (Dec. 22, 2014) [hereinafter Bitkower December 22 Comment Letter] (citing United States v. Karo, 468 U.S. 705, 718 (1984) (analogizing an NIT to installing a beeper in a container, where it is "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").

[131] David Bitkower, Deputy Assistant Attorney Gen., Additional Response to Comments Concerning Proposed Amendment to Rule 41, at 1 (Feb. 20, 2015) [hereinafter Bitkower February 20 Comment Letter].

[132] Bitkower December 22 Comment Letter, *supra* note 130, at 9.

[133] Bitkower February 20 Comment Letter, *supra* note 131, at 1; *cf.* 42 U.S.C. § 2000aa (2012).

[134] Bitkower February 20 Comment Letter, *supra* note 131, at 2.

[135] *See generally* Judicial Conf. Advisory Comm. on Crim. Rules, Pub. Hearing on Proposed Amendments to the Federal Rules of Criminal Procedure (Nov. 5, 2014), http://www.uscourts.gov/file/document/testimony-submitted-november-5-2014-hearing-proposed-amendments-federal-rules-criminal (providing the written testimonies submitted for the hearing).

[136] Comm. on the Rules of Practice and Procedure, Report of the Advisory Comm. on Criminal Rules, (May 6, 2015), *in* Final Materials for Congress 23, 24 [hereinafter Final Materials for Congress], http://www.uscourts.gov/file/document/2016-04-28-final-package-

in May 2015.[137] The Judicial Conference of the United States approved and submitted the amendments to the U.S. Supreme Court on October 9, 2015.[138] The Supreme Court followed suit in favor of the changes and forwarded the proposal to Congress in April 2016.[139] Congress could have rejected the amendments but failed to garner enough support to do so,[140] and Rule 41(b)(6) became authoritative on December 1, 2016.[141] The constitutional questions are left open, but these issues must be sorted out before widespread Fourth Amendment violations occur.[142]

IV. LARGEST KNOWN "REMOTE ACCESS" SEARCH IN FEDERAL LAW ENFORCEMENT HISTORY

"The difficulty of tactical maneuvering consists in turning the devious into the direct, and misfortune into gain."[143]

What started as a "Network Investigative Technique" to identify suspects involved in a vast online child pornography forum, later transcended United States' borders and came to be known as Operation Pacifier, the most extensive hacking investigation in law enforcement history.[144] Although the suspects apprehended in this operation do not satisfy a sympathetic profile, it has sparked

congress.

[137] Draft Minutes of Comm. on Rules of Practice and Procedure (May 28, 2015), *in* Comm. on Rules of Practice and Procedure Materials for Jan. 7–8, 2016 Meeting 31, http://www.uscourts.gov/sites/default/files/2016-01-standing-agenda-book.pdf.

[138] Memorandum from James C. Duff to the Chief Justice of the U.S. Supreme Court (Oct. 9, 2015), *in* Final Materials for Congress, *supra* note 136, at 212.

[139] *See* Letter from John G. Roberts, Chief Justice of the U.S. Supreme Court, to Paul D. Ryan, Speaker of the House of Representatives (Apr. 28, 2016), *in* Final Materials for Congress, *supra* note 136, at 200.

[140] For attempts to do so, see Stop Mass Hacking Act, S. 2952, 114th Cong. (2016), and its companion bill in the House, H.R. 5321, 114th Cong. (2016). Both explicitly rejected the amendments. *See* 162 CONG. REC. S. 3032–33 (daily ed. May 19, 2016) (statement of Sen. Wyden).

[141] *See* FED. R. CRIM. P. 41; *cf.* 28 U.S.C. § 2074(a) (2012) (providing that upon transmission to Congress, the rule shall take effect December 1 of that year, absent congressional action).

[142] FED. R. CRIM. P. 41 advisory committee's note to 2016 amendments ("The amendment does not address constitutional questions.").

[143] TZU, *supra* note 1, at 47.

[144] Stephen Montemayor, *Minnesotans Caught in FBI Child Porn Sting, Raising Constitutional Concerns*, STARTRIBUNE (Oct. 9, 2016, 7:58 PM), http://www.startribune.com/minnesotans-caught-in-fbi-child-porn-sting-raising-constitutional-concerns/396472281/; *see also* Joseph Cox, *Child Porn Sting Goes Global: FBI Hacked Computers in Denmark, Greece, Chile*, MOTHERBOARD (Jan. 22, 2016, 2:01 PM), http://motherboard.vice.com/en_us/child-porn-sting-goes-global-fbi-hacked-computers-in-denmarke-greece-chile.

a constitutional debate on how the FBI seeks out and apprehends criminals who hide in the obscurity of the Dark Net.[145] It was accomplished with a single website and a single warrant, which produced criminal defendants all over the country and confounded defense attorneys with a search on a scale they had never seen before.[146] What's more, some judges were unfamiliar with the technology employed by the FBI, which resulted in inconsistent application of constitutional law, and produced different results for defendants in different jurisdictions.[147]

A. *"Operation Pacifier—The Investigation and the Warrant*

According to the application for the search warrant, in September of 2014 agents began investigating a child pornography website operated on Tor's Dark Net, which had amassed 158,094 members and was visited weekly by over 11,000 unique users.[148] Rather than shut the site down, agents copied the contents of the website server and installed the website on a government facility in Newington, Virginia, where the FBI assumed administrative control and continued to operate it from a government-controlled server.[149] Agents proffered that the website was not easily accessed from a Google search, but rather, access to the site re-

[145] Ellen Nakashima, *This Is How the Government Is Catching People Who Use Child Porn Sites*, 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 (stating that the FBI's operation "is comparable to flooding a neighborhood with heroin in the hope of sharing an assortment of low-level drug users").

[146] *Id.*

[147] *See* Joseph Cox, *Judge in FBI Hacking Case Is Unclear on How FBI Hacking Works*, MOTHERBOARD (Jan. 27, 2016, 12:50 PM), http://motherboard.vice.com/read/judge-in-fbi-hacking-case-is-unclear-on-how-fbi-hacking-works; *see infra* Parts V and VI for recommendations on how to handle these situations.

[148] Application for a Search Warrant at 13, 18, *In re* Search of Computers that Access upf45jv3bziuctml.onion, No. 1:15-SW-89 (E.D. Va. Feb. 20, 2015) [hereinafter Operation Pacifier NIT Warrant], http://ia601205.us.archive.org/29/items/gov.uscourts.vaed.340813/gov.uscourts.vaed.340813.27.3.pdf. For coverage of this investigation, see also Mike Carter, *FBI's Massive Porn Sting Puts Internet Privacy in Crossfire*, SEATTLE TIMES (Aug. 27, 2016, 6:00 AM), http://www.seattletimes.com/seattle-news/crime/fbis-massive-porn-sting-puts-internet-privacy-in-crossfire/ (discussing Operation Pacifier, the subject website known as Playpen, and the litigation).

[149] *See* Operation Pacifier NIT Warrant, *supra* note 148, at 22–23; *see also* Joseph Cox, *The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers*, MOTHERBOARD (Jan. 5, 2016, 4:00 PM), https://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers (reporting that the FBI ran the website from its own servers from February 20 to March 4, 2015).

quired the web address obtained from other users, or finding the site from Internet postings describing the content available.[150]

In the warrant application, agents submitted that due to the anonymity provided by the nature of Tor's network, the IP address for the website, as well as the IP addresses of those visiting the site, could not be determined by a publicly available lookup or through a subpoena to the ISP. Thus, agents needed to "hack" or, as it is obliquely termed, employ an NIT.[151]

The NIT was "deployed on the [target website]" and "augment[ed] that content with additional computer instructions. When a user's computer successfully download[ed] those instructions . . . the NIT . . . caused the user's 'activating' computer to transmit certain information to a computer controlled by or known to the government."[152] The NIT then revealed identifying information to the government including: the activating computer's IP address, the type of operating system running on the computer (e.g., Windows), the "host name," the operating system username, and the MAC address.[153] The NIT was covertly passed from the website onto any computer—wherever located[154]—that logged into the website by entering a username and password, which in turn sent the identifying information to the government controlled computer.[155] This was a prototypical watering hole or drive-by-download tactic, whereby agents injected malware onto the website, so that when internet users accessed the site, the malware would be passed onto the website's visitor and the government could retrieve identifying information from that user's computer.[156]

Ostensibly, the warrant requested to search an unlimited number of unidentified computers—wherever located—but nevertheless, on February 20, 2015, a magistrate judge in the Eastern

[150] Operation Pacifier NIT Warrant, *supra* note 148, at 12.

[151] *See id.* at 11–12, 22–23. This is important in analyzing "reasonable expectations of privacy." *See infra* Part VI.

[152] Operation Pacifier NIT Warrant, *supra* note 148 at 24.

[153] *See id.* at 25.

[154] *Id.* at 29. Although the warrant application repeatedly refers to the fact that the government-controlled computer and website are operated from the Eastern District of Virginia, scrupulous review reveals that page 29 of the warrant application is the only place that agents imply that searches potentially will take place outside the issuing district. *See id.*

[155] *Id.* at 26.

[156] *See supra* Part II.B (discussing watering hole or drive-by-download tactics).

District of Virginia authorized the search warrant.[157] At the time, the website boasted 215,000 members, and pursuant to a single warrant, agents cast the NIT out into the sea of alleged suspects.[158] A remarkable 1300 IP addresses were returned, and armed with this information, agents all over the country secured a second warrant to search residences and arrest suspects.[159] The charges filed stemmed from this one warrant issued in the Eastern District of Virginia and led to an "escalating stream" of cases in nearly every state.[160]

B. *Defendants Challenged the Validity of the Warrant Across the Country*

The government employed its clandestine search methods on a massive scale, using technology that was ahead of constitutional law. Defendants filed motions to suppress, forcing federal district courts across the country to confront serious and complex legal issues for which there is no controlling circuit or Supreme Court precedent.[161] Courts came to markedly different conclusions, which will stand until further guidance can be offered by circuit courts and eventually, the Supreme Court.[162]

Nearly every district court found that the magistrate issuing the warrant exceeded her jurisdictional authority, and therefore, violated Rule 41(b).[163] Three jurisdictions suppressed all fruits of

[157] Operation Pacifier NIT Warrant, *supra* note 148, at 1.

[158] Cox, *supra* note 149; Nakashima, *supra* note 145.

[159] Cox, *supra* note 149; *e.g.*, Nakashima, *supra* note 145.

[160] *E.g.*, Cox, *supra* note 149 (quoting Colin Fieman, a public defender handling several cases).

[161] *See, e.g.*, United States v. Michaud, No. 3:15-CR-05351-RJB, 2016 U.S. Dist. LEXIS 11033, at *22 (W.D. Wash. Jan. 28, 2016); *see also* Montemayor, *supra* note 144 (quoting a Twin Cities attorney who has monitored Operation Pacifier cases across the country, stating that "[t]his is the place where constitutional law has not caught up with changes in technology").

[162] *E.g.*, United States v. Broy, No. 16-CR-10030, 2016 U.S. Dist. LEXIS 128616, at *1–2 (C.D. Ill. Sept. 21, 2016).

[163] *See, e.g.*, *id.* at *24; United States v. Croghan, No. 1:15-CR-48, 2016 U.S. Dist. LEXIS 127479, at *18 (S.D. Iowa Sept. 19, 2016); United States v. Torres, No. 5:16-CR-285, 2016 U.S. Dist. LEXIS 122086, at *16–17 (W.D. Tex. Sept. 9, 2016) (refusing to engage in judicial "finesse" to find the defendants had an "ethereal presence" in Virginia); United States v. Adams, No. 6:16-CR-11, 2016 U.S. Dist. LEXIS 105471, at *20 (M.D. Fla. Aug. 10, 2016); United States v. Werdene, No. 15-434, 2016 U.S. Dist. LEXIS 66311, at *2–3 (E.D. Pa. May 18, 2016); United States v. Arterbury, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67091, at *22 (N.D. Okla. Apr. 25, 2016); United States v. Levin, No. 15-10271, 2016 U.S. Dist. LEXIS 52907, at *17 (D. Mass. Apr. 20, 2016); *Michaud*, 2016 U.S.

the NIT Warrant.[164] A number of other courts found the NIT may have been unlawful, but suppression was unwarranted under the good faith exception; and three decisions from the Eastern District of Virginia and one from the Western District of Arkansas found that the magistrate acted within prescribed bounds of authority.[165] However, any discussion of the jurisdictional requirements under Rule 41 must be set aside given the recent amendments. What remains is the courts' splintered analysis of Fourth Amendment requirements as they apply to NIT warrants.

V. CONSTITUTIONAL FRAMEWORK FOR JUDGES CONSIDERING REMOTE ACCESS WARRANTS

"Ponder and deliberate before you make a move."[166]

It is crucial for the Fourth Amendment to keep stride with the inexorable pace of technology, or its protections will invariably be jettisoned. The Fourth Amendment states in relevant part that "no Warrants shall issue, but upon probable cause . . . particularly describing the place to be searched, and the persons or things to be seized."[167] These words, as interpreted by the U.S. Supreme Court, require three things to avoid amounting to an invalid warrant:[168] (1) "warrants must be issued by neutral, disinterested magistrates," (2) "those seeking the warrant must demonstrate to the magistrate their *probable cause* to believe that the evidence sought will aid in a particular apprehension or conviction for a particular offense," and (3) "warrants must particularly describe

Dist. LEXIS 11033, at *19. *But see* United States v. Jean, No. 5:15-CR-50087-001, 2016 U.S. Dist. LEXIS 123869, at *56 (W.D. Ark. Sept. 13, 2016) (holding that the warrant complied with Rule 41(b)(4)); United States v. Matish, No. 4:16-CR-16, 2016 U.S. Dist. LEXIS 82279, at *58–59 (E.D. Va. June 21, 2016) (holding that the warrant complied with Rule 41(b)(4)); United States v. Darby, No. 2:16-CR-36, 2016 U.S. Dist. LEXIS 74960, at *36 (E.D. Va. June 3, 2016) (holding that the warrant did not violate Rule 41(b)).

[164] *Croghan*, 2016 U.S. Dist. LEXIS 127479, at *22; *Arterbury*, 2016 U.S. Dist. LEXIS 67092, at *1 (adopting the magistrate judge's recommendation to suppress evidence arising from the NIT warrant); *Levin*, 2016 U.S. Dist. LEXIS 52907, at *40.

[165] *See Croghan*, 2016 U.S. Dist. LEXIS 127479, at *7–8.

[166] TZU, *supra* note 1, at 49.

[167] U.S. CONST. amend. IV.

[168] See Marcus v. Search Warrant of Prop., 367 U.S. 717, 724–29 (1961), for a summary of events in England and the early colonies that provided the background for the Fourth Amendment. The colonists abhorred unrestricted power of search and seizure which amounted to wide ranging "general warrants." *Id.* at 728.

the *things to be seized* as well as *the place to be searched.*[169] Federal law enforcement must satisfy these requirements to obtain a warrant for remote access searches, regardless of the information sought, because individuals have a reasonable expectation of privacy in any electronic device that stores personal information. Further, the surreptitious process of an NIT amounts to both a search and a seizure of the device.

A. *The Fourth Amendment Protects An Individual's "Reasonable Expectation of Privacy"*

Courts must decide whether inserting the NIT into computers is subject to Fourth Amendment protection, even when the only information sought is the discovery of IP addresses and other limited system related characteristics. The protections of the Fourth Amendment are preconditioned on whether the person invoking its guarantees can claim a justifiable, reasonable, or legitimate "expectation of privacy" in the place or thing to be searched.[170] This invokes two discrete inquiries: (1) whether the individual, by his conduct, has "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.'"[171] Therefore, the focal point is not on the items found, but rather on the area searched when inquiring whether a reasonable expectation of privacy exists.[172]

The caveat is that anything a person knowingly exposes to the public or voluntarily turns over to third parties is not subject to Fourth Amendment protection, and can be acquired without a warrant.[173] E-mail and internet users have been found to have no expectation of privacy in their e-mail addresses or the IP addresses of websites they visit because this information is inher-

[169] *E.g.*, Dalia v. United States, 441 U.S. 238, 255 (1979) (emphasis added).

[170] *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 950 (2012); Smith v. Maryland, 442 U.S. 735, 740 (1979) (collecting cases).

[171] *See, e.g.*, *Smith*, 442 U.S. at 740 (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan J., concurring)).

[172] *See* Rawlings v. Kentucky, 448 U.S. 98, 104–05 (1980); United States v. Horowitz, 806 F.2d 1222, 1224 (4th Cir. 1986)..

[173] *Smith*, 442 U.S. at 742–43 (holding no Fourth Amendment protection for phone numbers dialed and stored by phone company); *cf. Katz*, 389 U.S at 351–52 (finding privacy protection for phone calls placed in a public phone booth). The government can also acquire, without a warrant, items such as personal bank records. *See* United States v. Miller, 425 U.S. 435, 442–44 (1976).

ently provided to and used by ISP.[174] By contrast, jurisprudence underscores that an expectation of privacy exists in one's cell phone or personal computer because a search of such items would "expose to the government far *more* than the most exhaustive search of a house."[175]

B. *The District Courts Have Split on Whether Operation Pacifier's NIT Constituted a Search*

Courts are split on whether the Operation Pacifier NIT amounted to a search or not because they differ regarding whether the "expectation of privacy" inquiry is aimed at the object of the search, the computer, or at the information obtained, the IP address.[176] Some courts followed a pen register analogy to find that the warrant in Operation Pacifier was not needed because IP addresses are exposed to third parties and are not private.[177] One court went as far as finding there is no reasonable expectation of privacy in an IP address or a personal computer when agents are

[174] *E.g.*, United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008), *cert. denied sub nom.* Alba v. United States, 555 U.S. 908 (2008); *see also In re* United States for Historical Cell Site Data, 724 F.3d 600, 612 n.12 (5th Cir. 2013) (noting that the expectation of privacy is absent in IP addresses, e-mail addresses, phone numbers, and addressing information on the envelopes, to support the conclusion that there is no reasonable expectation of privacy in cell site data).

[175] *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2491 (2014); United States v. Otero, 563 F.3d 1127, 1132 (2009) (stating "the personal computer and its ability to store and intermingle a huge array of one's personal papers in a single place increases law enforcement's ability to conduct a wide-ranging search into a person's private affairs, and accordingly makes the particularity requirement that much more important").

[176] *Compare* United States v. Broy, No. 16-CR-10030, 2016 U.S. Dist. LEXIS 128616, at *16 (C.D. Ill. Sept. 21, 2016) (finding the defendant had a reasonable expectation of privacy in his computer, and thus, the NIT constituted a search), *and* United States v. Adams, No. 6:16-CR-11, 2016 U.S. Dist. LEXIS 105471, at *13–14 (M.D. Fla. Aug. 10, 2016), *with* United States v. Henderson, No. 15-CR-00565-WHO-1, 2016 U.S. Dist. LEXIS 118608, at *12–15 (N.D. Ca. Sept. 1, 2016) (finding no expectation of privacy in the IP address, and thus, the FBI could have legally discovered this information absent the NIT warrant), *and* United States v. Michaud, No. 3:15-CR-05351, 2016 U.S. Dist. LEXIS 11033, at *20–22 (N.D. Wash. Jan. 28, 2016) (likening the IP address to an unlisted telephone number and concluding the FBI could have obtained this without the NIT process).

[177] *See, e.g.*, United States v. Werdene, No. 15-434, 2016 U.S. Dist. LEXIS 66311, *24–26 (E.D. Pa. May 18, 2016); *Michaud*, 2016 U.S. Dist. LEXIS 11033, at *20–23; United States v. Matish, No. 4:16CR16, 2016 U.S. Dist. LEXIS 82279, at *70–71 (E.D. Va. June 21, 2016); United States v. Acevedo-Lemus, No. SACR 15-00137, 2016 U.S. Dist. LEXIS 105195, at *12–14 (C.D. Cal. Aug. 8, 2016) (concluding defendant had no expectation of privacy in his IP address while acknowledging that the FBI obtained defendant's IP address from his computer, not from a third party).

executing an NIT warrant.[178] That same court reasoned that the FBI exploiting a vulnerability by hacking a computer is akin to simply peering through broken blinds in an apartment.[179]

Still other courts found that (1) a Tor user has effectively disguised his IP address; (2) the NIT is necessary in order to discover this information; and (3) this is accomplished by surreptitiously planting malware on a defendant's computer.[180] These courts found that when agents inserted code onto the computers, they invaded the defendants' expectation of privacy in their computers.[181] In large part, the disparity in deciding this issue is due to a misunderstanding of anonymization technologies like the Tor network, and how the NIT functions.[182]

C. *Inserting NIT Code into A Computer Amounts to Both A "Search" and A "Seizure"*

Agents deploying an NIT are initiating a search within the meaning of the Fourth Amendment for three reasons. First, agents engage in a search when they use an NIT to discover a hidden IP address because, unlike an IP address obtained from a third party Internet service provider,[183] the FBI is only able to reveal the user's IP address by means of the NIT—and not through the traditional public look-up or subpoena served on a third party.[184] It is erroneous to conclude that when the IP address passes

[178] *See Matish*, 2016 U.S. Dist. LEXIS 82279, at *66–67, *73, *77 (reasoning that "in today's digital world, it appears to be a virtual certainty that computers accessing the Internet can—and eventually will—be hacked," and therefore, there is no expectation of privacy in a computer).

[179] *Id.* at *80. *But see Broy*, 2016 U.S. Dist. LEXIS 128616, at *17–18 ("Using the NIT to 'exploit a vulnerability in the online network' is not akin to police merely peering through broken blinds; it is akin to the police breaking the blinds and then peering through them.").

[180] *See, e.g.*, United States v. Arterbury, No. 15-CR-182, 2016 U.S. Dist. LEXIS 67091, at *28–30 (N.D. Okla. Apr. 25, 2016); United States v. Darby, No. 2:16CR36, 2016 U.S. Dist. LEXIS 74960, at *17–19 (E.D. Va. June 3, 2016); United States v. Torres, No. 5:16-CR-285, 2016 U.S. Dist. LEXIS 122086, at *9–10 (W.D. Tex. Sept. 9, 2016); United States v. Ammons, No. 3:16-CR-00011, 2016 U.S. Dist. LEXIS 124503, at *2 (W.D. Ky. Sept. 14, 2016).

[181] *See, e.g.*, *Arterbury*, 2016 U.S. Dist. LEXIS 67091, at *28–30; *see also supra* note 180 and accompanying sources.

[182] *See, e.g.*, *Michaud*, 2016 U.S. Dist. LEXIS 11033, at *21 (likening obtaining defendant's IP address to an unlisted telephone number); Cox, *supra* note 147.

[183] *See, e.g.*, United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008).

[184] Operation Pacifier NIT Warrant, *supra* note 148, at 11–12, 22–23; *Arterbury*, 2016 U.S. Dist. LEXIS 67091, at *29 n.10; *see also* United States v. Jean, No. 5:15-CR-50087-

through the first Tor node, a disclosure to a third party occurs[185] because it is one of thousands of randomly routed nodes in the Tor network and each node only knows its successor and predecessor—not the original sender.[186] Agents would still need to deploy the NIT in order to discover computer system information.[187] Indeed, the FBI admits in its application the inability to discover the IP addresses and their dependence on the NIT.[188] Thus, a computer user's identifying information no longer falls within the category of information "disclosed to third parties" when employing anonymization technology, and therefore, the FBI must secure a warrant before executing an NIT.[189] *Kyllo v. United States* holds that when the government uses a device that is not in general public use, to discover information that would previously have been unknowable without physical intrusion, the surveillance is a search and is presumptively unreasonable without a warrant.[190] Remotely deploying computer malware may fairly be categorized as not in general public use, and requires judicial authorization. A contrary determination would open the door to unmitigated government surveillance that would circumvent society's privacy measures.[191]

Second, executing an NIT is a search because when NIT code is planted on a dark website that is accessed by a user whose address is disguised through Tor, the NIT in reality does more than simply discover the IP address. Specifically, this is because (1) by

001, 2016 U.S. Dist. LEXIS 123869, at *28 n.14 (W.D. Ark. Sept. 13, 2016) (noting that the IP address was not obtained from a third party).

[185] United States v. Werdene, No. 15-434, 2016 U.S. Dist. LEXIS 66311, at *27 (E.D. Pa. May 18, 2016).

[186] Owen & Savage, *supra* note 50, at 1; Dingledine et al., *supra* note 52, at 1.

[187] This is because deanonymizing Tor users requires advanced technical capabilities and an immense amount of time. *See* Caliskan et al., *supra* note 38, at 13–15.

[188] Operation Pacifier NIT Warrant, *supra* note 148, at 11–12, 22–23.

[189] *See* United States v. Forrester, 512 F.3d 500, 505 (9th Cir. 2008). In that case, the IP address was obtained from PacBell's connection facility, and in *United States v. Caira*, the IP address was obtained from Microsoft by subpoena. *Id.*; 833 F.3d 803, 805–09 (7th Cir. 2016). These are prominent distinctions of how an IP address is obtained through use of an NIT. This in turn alters the "reasonable expectation of privacy" analysis because a third party cannot provide officers with a Tor user's system identifying information.

[190] Kyllo v. United States, 533 U.S. 27, 40 (2001). Although *Kyllo* involved officers using thermovision to see through the walls of a home, a search of a computer or cell phone is likely far more threatening. *See* Riley v. California, 134 S. Ct. 2473, 2491 (2014) ("[A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house.").

[191] Additionally, a proliferation of illegal activity, like hacking and computer abuse, should not form the basis of "in general public use" in order to allow agents to forego warrant requirements.

using Tor a user does not disclose their IP address, so even the IP address is private, and (2) by obtaining the user's IP address as a result of the user triggering the NIT on the illicit web page, the FBI is able to connect the address to the incriminating web page. As a result, the FBI obtains the confidential fact that the IP address holder sought specific information.[192] This makes an NIT less like a pen register (a device that records numbers dialed from a phone line)[193] and more like a wiretap, which would disclose that the suspect sold child porn on the phone call.[194]

Third, the Fourth Amendment protects property as well as privacy,[195] and an NIT is a search because the NIT code "physically occupie[s] private property for the purpose of obtaining information."[196] In *United States v. Jones*, the Supreme Court held that the government's installation of a GPS device on a target vehicle was a search because the device occupied physical space for the purpose of obtaining information.[197] Similarly, in *Florida v. Jardines* the Court found that an officer and his drug-sniffing canine simply standing on the porch of a residence to detect the presence of narcotics was a search because the officer physically entered a private area to engage in conduct not authorized by the homeowner.[198]

The NIT in Operation Pacifier was malware code written into a web page and passed onto a user's computer.[199] The contents of a computer is simply code, and just like attaching a GPS device to a car in *Jones*, the code of an NIT occupies physical space on a computer, which is constitutionally protected property,[200] and the

[192] *See* Operation Pacifier NIT Warrant, *supra* note 148, at 5 (declaring that the NIT will reveal "the 'activating' computer's actual IP address, and the date and time that the NIT determines what the IP address is"). By definition, if the NIT is triggered and the IP address revealed, the user has visited the dark web page.

[193] Smith v. Maryland, 442 U.S. 735, 736 n.1 (1979) (defining a pen register as a mechanical device, usually installed at a telephone facility, that records the numbers dialed on a telephone but does not record communications or whether the call was completed).

[194] *See* 18 U.S.C. § 2510(4) (2016) (defining "intercept" to mean "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device").

[195] *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 949 (2012).

[196] *Id.*; *see also* Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013).

[197] 132 S. Ct. at 948–49.

[198] 133 S. Ct. at 1413–14.

[199] *See* Cova et al., *supra* note 76, at 281; Rid & Buchanan, *supra* note 62, at 16.

[200] Riley v. California, 134 S. Ct. 2473, 2491 (2014); United States v. Otero, 563 F.3d 1127, 1132 (2009).

NIT serves the purpose of obtaining information not authorized by the owner. Indeed, at least one district court followed this rationale and reasoned that the trespassory nature of inserting NIT code onto the computers of those who visit a web page constitutes a search.[201]

Finally, an NIT also constitutes a temporary seizure of a user's computer. *United States v. Place* instructs that a seizure does occur when, without consent, agents temporarily take private property to conduct a search.[202] *Place* stands for the principle that government control of private property does not have to be permanent to be a seizure. Just as the luggage in *Place* was seized, so too is a target computer seized with NIT malware, because once the user visits the watering hole, the web page forces the computer to download the NIT code, store it, and execute the malicious application, which controls the computer and directs it to return system identifying information to FBI agents.[203] By taking control of a user's computer, even temporarily, to direct it to provide information unobtainable in any other way, the NIT seizes the computer without authorization from the user.[204]

It is the object of the search that is pertinent, not the information obtained.[205] The fact that an internet user may not have an expectation of privacy in an IP address is of no relevance because the NIT process involved in obtaining that information involves invading a computer and planting code that occupies space, which seizes control of the device in order to compel it to reveal its identifying information. Thus, agents must satisfy

[201] *See* United States v. Darby, No. 2:16CR36, 2016 U.S. Dist. LEXIS 74960, at *19 (E.D. Va. June 3, 2016).

[202] 462 U.S. 696, 707 (1983); *see also* Illinois v. Caballes, 543 U.S. 405, 409–10 (2005) (holding that a canine sniff on the exterior of the vehicle during a traffic violation stop does not violate the Fourth Amendment because it is within the scope of the stop and reveals no more than the presence of illegal contraband).

[203] *See* Lu et al., *supra* note 76, at 440–41; *see also* Operation Pacifier NIT Warrant, *supra* note 148, at 24–25. The argument that an NIT is more like a lawful "canine-sniff" because it merely detects the presence of contraband, breaks down because unlike detecting the presence of narcotics in luggage clearly in plain view, neither a user's computer nor the IP address is exposed to public view at the time of the search. *See Place*, 462 U.S. at 697–98, 707.

[204] *See* United States v. Arterbury, No. 15-CR-182, 2016 U.S. Dist. LEXIS 67091, at *30; *Darby*, 2016 U.S. Dist. LEXIS 74960, at *18–19.

[205] *See, e.g.*, United States v. Horowitz, 806 F.2d 1222, 1224 (4th Cir. 1986); Rawlings v. Kentucky, 448 U.S. 98, 104–05 (1980). For example, an individual does not have a legitimate expectation of privacy in a stolen vehicle. *See* United States v. Soto, 779 F. Supp. 2d 208, 218 (2011). However, when government action invades a home to search for that vehicle, a warrant is required. Silverman v. United States, 365 U.S. 505, 511–12 (1961).

Fourth Amendment proscriptions for obtaining a warrant prior to executing remote access searches.

VI. ANALYZING PROBABLE CAUSE AND PARTICULARITY FOR "NIT" WARRANT APPLICATIONS

"[I]n the wise leader's plans, considerations of advantage and of disadvantage will be blended together."[206]

A search warrant that authorizes an NIT to be launched from a website is not a search of one or two computers; it implicates thousands of internet users' electronic devices. The gravity of the search is compounded by the reality that the targets of the search are unknown, and therefore the website itself, as the only known factor, must play a substantial role in the Fourth Amendment analysis.[207] Deliberation and forethought is vital to making a narrow determination that there is probable cause for each internet user that may potentially visit the site in question. This involves considering whether there are legal or innocuous purposes for visiting the site, as well as the potential for searching unintentional visitors. Should a magistrate reasonably determine that each user visiting the website is engaged in the unlawful activity, then a single warrant to search thousands of computers is justified.[208]

A. *The Warrant Requirements: Probable Cause & Particularity in Operation Pacifier*

The underpinnings of the Fourth Amendment have two interests at heart. First, because "*any* intrusion in the way of a search or seizure is an evil," the probable cause requirement permits only those searches founded on a careful predetermination that evi-

[206] TZU, *supra* note 1, at 54.

[207] Scholars have offered that the particularity requirement should apply to internet users, not accounts, because the suspect is the one constant in the physical and virtual world. *See* Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1045–46 (2010). However, if the suspects are unknown, and the website allows for criminals and naïve users to access the site, the website becomes the driving force for determining probable cause, which will govern the requisite particularity.

[208] Information that cocaine dealers will be making sales among the spectators at a sports arena would hardly justify searching each member of the crowd. Likewise, presence at a dark website, without more, is unlikely to establish probable cause.

dence, instrumentalities, fruits of a crime, or contraband will be found.[209] Second, to prevent the "exploratory rummaging in a person's belongings,"[210] the particularity requirement ensures that a search will be carefully tailored to its justifications, and will not become "the wide-ranging exploratory searches the Framers intended to prohibit."[211] These two requirements are intertwined and work in tandem to limit law enforcement's authorization to search in specific areas, for specific things in which there is probable cause to search.

The probable cause component is a fluid concept, which turns "on the assessment of probabilities in particular factual contexts."[212] By contrast, the requisite particularity for a warrant is more exacting. The warrant must set out with "particular[ity] . . . the place to be searched and the persons or things to be seized."[213] The calculus for determining probable cause is then an inquiry applied to each place to be searched and each item to be seized.[214]

"The NIT Warrant [in Operation Pacifier] describes particular places to be searched—computers that have *logged into [the website]*—for which there was probable cause to search."[215] The courts consistently found that the scope of probable cause satisfied the particularity of the warrant given the alarming and pervasive content of the website.[216] In large part this was due to the "nu-

[209] *See* Coolidge v. New Hampshire, 403 U.S. 443, 467 (1971); Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 301–02 (1967).

[210] *Coolidge*, 403 U.S. at 467.

[211] Maryland v. Garrison, 480 U.S. 79, 84 (1987).

[212] Illinois v. Gates, 462 U.S. 213, 232 (1983). An inherent realization should be that innocent behavior often will provide the basis for probable cause, otherwise a more stringent standard would be imposed than our security demands. *See id.* at 243 n.13. *But see* Brown v. Texas, 443 U.S. 47, 52 (1979) (discussing how the fact that a scenario "looked suspicious" was not enough).

[213] *See* CONST. amend. IV; FED. R. CRIM. P. 41(e)(2)(A) (a warrant "must identify the person or property to be searched, identify any person or property to be seized").

[214] *See Garrison*, 480 U.S. at 84.

[215] United States v. Darby, No. 2:16CR36, 2016 U.S. Dist. LEXIS 74960, at *27–28 (E.D. Va. June 3, 2016) (emphasis added); *see, e.g.*, United States v. Broy, No. 16-CR-10030, 2016 U.S. Dist. LEXIS 128616, at *9 (C.D. Ill. Sept. 21, 2016); United States v. Michaud, No. 3:15-CR-05351, 2016 U.S. Dist. LEXIS 11033, at *9–12 (W.D. Wash. Jan. 28, 2016).

[216] *See, e.g.*, United States v. Matish, No. 4:16CR16, 2016 U.S. Dist. LEXIS 82279, at *33–37 (E.D. Va. June 21, 2016); United States v. Acevedo-Lemus, No. SACR 15-00137, 2016 U.S. Dist. LEXIS 105195, at *22 n.4 (C.D. Cal. Aug. 8, 2016) (noting that the particularity argument has been rejected by nearly every court to consider it). *But see In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d at 755–58 (2013) (finding a warrant to "surreptitiously install[] software designed . . . to extract

merous affirmative steps" and "the complicated machinations through which users had to go to access the web site (meaning that unintentional users were unlikely to stumble onto it)."[217]

B. *Probable Cause and Particularity Regarding Unknown Computer Users*

There is untold investigative potential in executing NIT warrants, and with the best intentions it could be used to thwart foreign and domestic terrorist plots and large scale attacks on United States' economic interests. Our society ought to aggressively pursue all such crimes, particularly those such as the appalling crimes involving child abuse imagery. However, viewing online child pornography is a one-of-kind crime because merely accessing the website may constitute culpable activity.[218] Regardless of the crime being investigated, courts must be cautious about the precedent set regarding how broadly the FBI can use NIT technology. In Operation Pacifier agents used a child pornography website to search thousands of unknown computers across the nation with a single warrant, but this tactic could easily be utilized on more benign websites. This result can be avoided by evaluating the website in the same way a determination would be made to search all persons inside a large building where there is ongoing suspected illegal activity.

1. The "All Persons" Warrant

The government's use of a watering hole to deploy an NIT represents the vanguard of the FBI's hacking campaign. A single warrant to search so broadly is unheard of.[219] However, there is a stringent, albeit rare, scenario in the case of physical searches

certain stored electronic records" from "an unknown computer at an unknown location" did not satisfy Fourth Amendment particularity requirement).

[217] *See* United States v. Epich, No. 15-CR-163, 2016 U.S. Dist. LEXIS 32459, at *3 (E.D. Wis. Mar. 14, 2016); *Matish*, 2016 U.S. Dist. LEXIS 82279, at *33, *37; *Michaud*, 2016 U.S. Dist. LEXIS 11033, at *14 (stating that it "would be highly unlikely that Website A would be stumbled upon").

[218] *See, e.g.*, 18 U.S.C. § 2252A(a)(5)(B) (2012) (establishing the crime to "knowingly access, with intent to view . . . child pornography").

[219] *See* Cox, *supra* note 149 (quoting Christopher Soghoian, principle technologist at the ACLU). "We're talking about the government hacking thousands of computers, pursuant to a single warrant,"—likely the largest law enforcement hacking campaign to date. *Id.*

that can be applied to NIT warrants, known as the "all persons" warrant. The seminal case to present the viability of a warrant to search all persons found at a given location was *State v. De Simone*.[220] That case involved a warrant to search a vehicle and "all persons found therein" for lottery slips.[221] The *De Simone* court upheld the conviction and forged the following language that is quoted by numerous jurisdictions:

> On principle, the sufficiency of a warrant to search persons identified only by their presence at a specified place should depend upon the facts. A showing that lottery slips are sold in a department store or an industrial plant obviously would not justify a warrant to search every person on the premises, for there would be no probable cause to believe that everyone there was participating in the illegal operation. On the other hand, a showing that a dice game is operated in a manhole or in a barn should suffice, for the reason that *the place is so limited* and the *illegal operation so overt* that it is likely that everyone present is a party to the offense. Such a setting furnishes not only probable cause but also a designation of the persons to be searched which functionally is as precise as a dimensional portrait of them . . . .
>
> So long as there is good reason to suspect or believe that anyone present at the anticipated scene will probably be a participant, presence becomes the descriptive fact satisfying the aim of the Fourth Amendment. The evil of the general warrant is thereby negated. To insist nonetheless that the individual be otherwise described when circumstances will not permit it, would simply deny government a needed power to deal with crime, without advancing the interest the Amendment was meant to serve.[222]

Although the "all persons" warrant has never directly been addressed by the Supreme Court,[223] the issue of a warrant to search "all persons" has since been addressed in approximately forty-three jurisdictions, with eight holding that it was unconstitutional, and at least another thirty following the *De Simone* ra-

[220] 288 A.2d 849 (N.J. Sup. Ct. 1972).

[221] *Id.* at 850.

[222] *Id.* at 850–51 (emphasis added). For a collection of cases quoting *De Simone*, see Marks v. Clarke, 102 F.3d 1012, 1029 (9th Cir. 1996); Baker v. Monroe Twp., 50 F.3d 1186, 1198–99 (3d Cir. 1995); United States v. Guadarrama, 128 F. Supp. 2d 1202, 1207–08 (E.D. Wis. 2001); State v. Boyer, 967 So. 2d 458, 465 (La. 2007).

[223] *See* Ybarra v. Illinois, 444 U.S. 85, 88–89, 92 n.4 (1979). In *Ybarra*, a warrant was issued to search a bartender and one other person, at a tavern where there was substantial drug activity. *Id.* at 87–89. Police proceeded to pat down all within the bar. *Id.* at 88. The court held the search was unconstitutional because "a warrant to search a place cannot normally be construed to authorize a search of each individual in that place." *Id.* at 92 n.4.

tionale.[224] *De Simone*'s rationale has also been endorsed by leading constitutional scholars, reasoning that a search for "all persons present" at a given location may be constitutional following cautious review of the nature of the location and the unlawful activity.[225]

For example, in *State v. Hinkel*, a warrant was upheld for the search of "all persons on the premises" of an "afterhours joint" because probable cause supported that "[t]here was little likelihood that anyone would be in the house but to participate in the afterhours revelry."[226] Similarly, warrants have been upheld to search "any and all persons found upon said premises . . . with the exception of people who may arrive upon or be upon said premises in a regular course of business, (i.e., postman, delivery people)" because there was probable cause that evidence of a crime would be found through a search of anyone present at the defendant's residence at the time of the search.[227]

In stark contrast, the Ninth Circuit addressed the search of an entire Gypsy Church rejecting the "den of thieves" argument to justify a search of all persons simply because they were there. The court found that the warrant was insufficiently particular because it permitted a search of "any persons on the premises," which would have included innocent children and family members.[228] Similarly, the Supreme Court of Iowa deemed a warrant to search "[a]ll persons located inside the premises" to be overbroad despite that the reputation of the bar "is such that no local people would enter without the intention to purchase or sell controlled substances."[229] The court reasoned that "it is a *legally* operated, legitimate business . . . it is still quite possible someone from out of town or new to the area could stop in to ask directions, use a pay phone, or make a legal purchase."[230] Even

[224] *See Guadarrama*, 128 F. Supp. 2d at 1207, n.3–4. Further, three states have held or expressed in dicta that "all persons" warrants are unconstitutional general warrants; five other jurisdictions find that such warrants do not provide a sufficiently particular description under the Fourth Amendment. *Id.* at 1207.

[225] *See* 2 WAYNE R. LAFAVE, SEARCH AND SEIZURE: A TREATISE ON THE FOURTH AMENDMENT § 4.5(e) (5th ed. Oct. 2016) (endorsing the limited rationale outlined in *De Simone* as the proper analysis for "all persons present" warrants).

[226] 365 N.W.2d 774, 775–77 (Minn. 1985).

[227] State v. Allard, 674 A.2d 921, 922–23 (Me. 1996).

[228] Marks v. Clarke, 102 F.3d 1012, 1015, 1028–29 (9th Cir. 1996). The affidavit only supported probable cause to search two individuals). *Id.* at 1028.

[229] State v. Thomas, 540 N.W.2d 658, 665–66 (Iowa 1995).

[230] *Id.*

warrants to search "any and all vehicles and persons present at the scene" of a residence allegedly engaged in ongoing drug sales and use have been struck down because this implicates "every vehicle at a family home, during daytime hours, when unsuspecting friends, neighbors, or laborers could be present."[231]

De Simone and similar cases addressing a warrant to search "all persons" at a given place support the proposition that even ongoing and pervasive criminal conduct at a suspected location does not negate the fact that law abiding citizens may be engaged in legal activities at the locality. Yet in certain circumstances a warrant may be issued to search "all persons" found on a premises—persons who ultimately are unknown at the time of issuance.[232] However, the risk that an innocent person may be swept up in a dragnet search is a part of the careful calculus of the Fourth Amendment's requirements.[233]

C. *Limiting the Sting of Rule 41—Applying* De Simone *to Applications for NIT Warrants*

De Simone takes into consideration the reality that a search of everyone found on a premises will likely include law abiding citizens, and accounts for this by requiring an expansive scope of the probable cause element to justify equally broad particularity. The Supreme Court has recognized that digital devices, like cell phones, are "capable of storing and accessing a quantity of information, some highly personal, that no person would ever have had on his person in hard-copy form."[234] For this reason, the same considerations and requirements of an "all persons" search should apply with equal force in the search of "all computers" visiting a target website because presumably innocent parties may be caught in the government's watering hole search tactic. Courts are willing to require probable cause that evidence of a crime will

[231] United States v. Swift, 720 F. Supp. 2d 1048, 1055, 1057–58 (E.D. Ark. 2010).

[232] *See* State v. Hinkel, 365 N.W.2d 774, 777–76; *Allard*, 674 A.2d at 922–23.

[233] *See* United States v. Guadarrama, 128 F. Supp. 2d 1202, 1208 (E.D. Wis. 2001) (stating, "the question is whether there is sufficient particularity in the probable cause sense, that is, whether the information supplied the magistrate supports the conclusion that it is probable anyone in the described place when the warrant is executed is involved in the criminal activity in such a way as to have evidence thereof on his person") (quoting LAFAVE, *supra* note 225).

[234] Riley v. California, 134 S. Ct. 2473, 2495, 2496 (2014) (Alito, J., concurring).

likely be found on each person found on the premises,[235] and thus, the same standard should apply to "all computers" accessing a dark website because the later, a search of one's computer, is likely to be an even more invasive search.[236]

Agents deploying NITs, or malware techniques, from a website in a watering hole scenario should be required to demonstrate that the unlawful website content is of such a pervasive nature, like a site dedicated to child pornography, that it is extremely unlikely that one would enter for an innocuous purpose. Many sites may fall into the repugnant category and others may contain unpalatable chat groups or comment feeds, but a site often is not entirely devoid of lawful purpose. The potential for innocent and legal activity on any given site, as well as, the potential for inadvertent visitors, must be taken into consideration. "[A] person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person."[237] It follows that a person's mere presence on a website is unlikely to afford probable cause to search their computer. Tribunals must determine the overt and conscious acts required to access the site, even for a site that is so rife with illegal purpose. This ensures that happenstance does not ensnare the unsuspecting internet surfer in the ploy of an NIT search warrant.

Secondly, in investigations involving a botnet controlled by a master, a search of all computers unknowingly infected with the malware will hardly be grounds for probable cause, given that a botnet is by definition—controlled by one or a few criminals.[238] The mere fact that one's computer has been commandeered by a botmaster to perpetuate online crime does not support probable cause to search each computer because this does not constitute involvement in unlawful activity. Searching botnet victims would be analogous to searching recently liberated victims of a hostage situation and filing charges based on the evidence obtained.

[235] *See, e.g.*, *Swift*, 720 F. Supp. 2d at 1056 (citing Owens v. Lott, 372 F.3d 267, 276 (4th Cir. 2004)).

[236] *See Riley*, 134 S. Ct. at 2491 ("[A] cell phone search would typically expose to the government far *more* than the most exhaustive search of a house.").

[237] Ybarra v. Illinois, 444 U.S. 85, 91 (1979) (citing Sibron v. New York, 392 U.S. 40, 62–63 (1968)).

[238] *See supra* Part II.D.

A warrant in a botnet investigation is only likely to be authorized for the purpose of the government removing malware from the infected computer, and the scope of such a warrant will not permit agents to rummage through the hard drive of each computer. Many may be innocently and involuntarily linked to the master of the botnet, and such a nexus does not warrant an "all computers" search.

D. *Recommended Criteria for Evaluating a Search of "All Computers" Accessing a Site*

An "all computers" search warrant should be "authorized under the Fourth Amendment only if the supporting affidavit establishes probable cause that evidence of illegal activity will [likely] be found upon every person to fall within the warrant's scope at the time of execution."[239] Warrants that pass constitutional muster will likely only reach those engaged in culpable online activity.

First, in order for government agents to deploy an NIT, the site should be hidden, unavailable through a general Google search, or bear an apparently offensive URL. This is necessary to prevent stumbling upon the site,[240] and triggering the NIT search upon merely landing on the homepage. Second, the site to be injected with malware should be one that requires registration or an invite from website members. Third, the website must serve an ostensibly illegal purpose and the content purporting to do so must be pervasive throughout the site.

Fourth, and most importantly, agents should reasonably limit the scope and probability of ensnaring those stumbling upon the site by planting the NIT code, not on the home page, but further within the website so that an individual's happenstance encounter with the site does not trigger the search. Agents must embed the malware code deeper within the website.[241] These four requirements would operate similarly to the minimization require-

[239] *See Swift*, 720 F. Supp. 2d at 1056. Those concerned about the government's reach under Rule 41 can rest assured because if this standard is followed, warrants likely to satisfy these standards are few.

[240] *See* Rid & Buchanan, *supra* note 62, at 16.

[241] Suggested options may include the images portion of a web page, or in the case of online black markets, at the checkout page. In this manner, there is good reason to believe that at that point an individual has no longer mistakenly visited the site, but engaged in illegal activity and overtly moved to complete the crime.

ments for wiretap surveillance,[242] to ensure that like wiretaps, NITs "shall be conducted in such a way as to minimize" the number of computers subject to search.[243] These four factors are indicia of probable cause to believe that each user accessing the target site is involved in the illegal activity.

This criterion should find favor with the courts as well as the critics of Rule 41 because it allows law enforcement to efficiently search for evasive online criminal activity, while still protecting the interests of those naïvely or curiously searching the Internet. For example, similar to a bar with a reputation for attracting reprehensible characters who distribute narcotics,[244] a jihadi website may well offer unlawful services and discuss egregious acts. However, just as the bar may occasionally provide a patron with the opportunity to make a legal purchase, so too does a facially unsettling website provide a resource for journalists and researchers alike.[245] This militates in favor of requiring that probable cause be demonstrated for each person that will visit a website deploying an NIT.[246]

Rule 41(b)(6) affords the potential for limitless reach. There is little recourse for Fourth Amendment violations due to substantial social costs, and excluding evidence "has always been [the courts'] last resort, not [its] first impulse."[247] Considering that warrant applications are conducted ex parte, the mantle then

[242] *See* United States v. Donovan, 429 U.S. 413, 435 (1977) (citing 18 U.S.C. §§ 2518(3)(a–d) (2012)).

> The issuing judge may approve an intercept application if it is determined that normal investigative techniques failed or are unlikely to succeed and there is probable cause to believe that: (i) an individual is engaged in criminal activity; (ii) particular communications concerning the offense will be obtained through interception; and (iii) the target facilities are being used in connection with the specified criminal activity).

See id.

[243] *See* 18 U.S.C. § 2518(5) (2012).

[244] *See* State v. Thomas, 540 N.W.2d 658, 665–66 (Iowa 1995).

[245] By definition, agents will be unable to determine if the computers being searched belong to a newspaper or media station given that many journalists' computers are "concealed through technological means." *See* FED. R. CRIM. P. 41(b)(6)(A); *see also* Caliskan et al., *supra* note 38, at 24 (listing a myriad of groups who conceal the location of their computers); Jardine, *supra* note 36, at 5 (articulating that anonymity is part of a journalists "survival kit").

[246] Inadvertently searching computers used for newsgathering would likely contravene statutory authority. See Privacy Protection Act of 1980, 42 U.S.C. § 2000aa(a) (2012), passed in response to *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978).

[247] Herring v. United States, 555 U.S. 135, 140 (2009) (quoting Hudson v. Michigan, 547 U.S. 586, 591 (2006)).

rests on the judiciary at the outset to protect Fourth Amendment interests and curtail NIT warrants that seek to overreach. Otherwise, the FBI's methods could easily extend to searches launched from progressive Islamic and jihadi websites, but there are legitimate reasons journalists and reporters visit such sites while using anonymization technology.[248] Magistrates must proceed with caution and target their Fourth Amendment inquiry on the circumstances surrounding the website. A careful evaluation must be undertaken as to the mechanics, nature and content of the site to ensure that there is indeed probable cause to search potentially every computer in the nation that visits the site in question.[249]

E. *The Means of Executing the Remote Access Warrant Must Be Reasonable*

Even when agents have properly secured a warrant to conduct a search, the method of entry is one factor to be considered in assessing the reasonableness of a search and/or seizure.[250] *Wilson v. Layne* instructs that even if agents hold a valid warrant, when it is executed with third parties present who do not aid in the execution of the warrant a search may be rendered unreasonable.[251]

Executing an NIT differs from simply entering into a home. Malware hacking technology is not perfect, and the process involves law enforcement exploiting vulnerabilities in a system.[252] When law enforcement opts for this practice they risk allowing criminals to hijack legitimate government searches or reverse engineer government malware.[253] For example, in 2011 the largest

[248] *See, e.g.*, Jardine, *supra* note 36, at 5.

[249] If the search will involve capturing video or similar forms of surveillance, more exacting Fourth Amendment standards outside those outlined in this piece should be applied. *See, e.g.*, United States v. Cuevas-Sanchez, 821 F.2d 248, 251–52 (5th Cir. 1987) (adopting 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 (2012)).

[250] Wilson v. Arkansas, 514 U.S. 927, 934 (1995).

[251] Wilson v. Layne, 526 U.S. 603, 611–14 (1999) (involving reporters invited to witness the search); Hanlon v. Berger, 526 U.S. 808, 809–10 (1999) (involving a media "ride along").

[252] *See* Rid & Buchanan, *supra* note 62, at 16; INTERNET SECURITY THREAT REPORT, *supra* note 64, at 62–63.

[253] *See* Ron Wyden, Matt Blaze, & Susan Landau, *The Feds Will Soon Be Able to Legally Hack Almost Anyone*, WIRED (Sept. 14, 2016, 7:00 AM), https://www.wired.com/2016/09/government-will-soon-able-legally-hack-anyone/ (providing examples of hackers

European hacker club reverse engineered a lawful interception malware program to provide a functional backdoor to anyone on the Internet, which allowed hackers to remotely control computers and activate microphones and cameras.[254] This not only jeopardizes the security of those searched but puts government search tools in the hands of criminals who can then turn them on government and private sector computer systems.[255]

By creating doors that other hackers can use, the FBI's NIT malware creates a scenario far more unreasonable than just inviting the media for a ride along.[256] This situation is more like the FBI offering tours of the investigation scene to those passing by and handing out copies of the keys to the front door as they come through. If the risks of executing malware are properly understood, this is more than a policy problem; it's a Fourth Amendment problem that should govern the execution of remote access warrants.

However, while criminals still have to find the back door created by agents, the government may have created a permanent open-door policy for its agents because once the NIT code is on a computer system—how is it removed? What capabilities does the government have once an NIT has been deployed on a target computer?[257] Answers to these questions are unlikely to come out in the ex parte warrant process. Therefore, courts ought to err on the side of caution and minimize the number of NIT warrants

getting ahold of law enforcements techniques); *see also* Dan Goodin, *Root Backdoor Found in Surveillance Gear Used by Law Enforcement*, ARS TECHNICA (May 28, 2014, 3:11 PM), http://arstechnica.com/security/2014/05/root-backdoor-found-in-surveillance-gear-used-by-law-enforcement/ (detailing a litany of critical weaknesses in government surveillance).

[254] *Chaos Computer Club Analyzes Government Malware*, CHAOS COMPUTER CLUB (Oct. 8, 2011), http://ccc.de/en/updates/2011/staatstrojaner; *see also* Second ACLU Comment, *supra* note 120 at 9.

[255] *See* Pell, *supra* note 28, at 532–34 (examining the dangers of creating "back doors" in communications systems that could be exploited to allow improper access by organized crime operations, and there "is no way to create a back door that will work only for legitimate surveillance"). These same concerns apply when the "door" is surreptitiously created by agents hacking a computer with malware.

[256] *Wilson*, 526 U.S. at 604, 614; *Hanlon*, 526 U.S. at 809–10.

[257] *See* Operation Pacifier NIT Warrant, *supra* note 148, at 28. This provides little insight and states only that the "NIT will be used on the TARGET WEBSITE for not more than 30-days." *See also In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 755 (S.D. Texas 2013) (explaining that here, the government's software had the capacity to search the computer's hard drive, activate the computer's built-in camera, generate latitude and longitude coordinates for the computer's location, and to transmit the extracted data to FBI agents).

granted by requiring that applications meet the prophylactic criterion outlined in this comment.

CONCLUSION

"Be stern in the council-chamber, so that you may control the situation."[258]

The judiciary faces the arduous task of familiarizing itself with the technology involved in remotely accessing a computer through an NIT, as NIT warrants will become much more commonplace now that Rule 41 no longer obstructs law enforcement. Fourth Amendment requirements will need to be strictly applied to prevent combing searches across the Internet.

If the constitutional construct outlined in this comment is followed for an all computers search, law enforcement will be successful in capturing those engaged in illegal activities in the shadows of the ether. This involves evaluating probable cause for all computers visiting a website, in the same manner that probable cause would be assessed for all persons found on a premises—by determining the potential for innocent bystanders being caught in the search.

The scope of the crime does not necessarily need to limit the scope of the investigation. The particularity of the warrant may allow for a search of computers in all ninety-four districts, if probable cause is broad enough to support this finding. This settles the apprehension as to how Fourth Amendment requirements and Rule 41(b)(6) can coexist, while allowing law enforcement to combat cybercrime on equal footing. Moreover, the online markets for criminal paraphernalia, as well as the remote and far-reaching cyber attacks on United States' interests will now face duly authorized law enforcement.

Those who are engaged in internet crimes will indeed have reason to fear, as law enforcement will have the tools and territorial capacity to implement its investigations. The general populous will not be forced to choose between privacy and security. Those citizens seeking to remain anonymous, who have otherwise been law abiding, may keep aspects of their lives private and will not

[258] TZU, *supra* note 1, at 81.

be caught in the wake of a general search. The updated Rule 41 will only result in an invasion of privacy if the judiciary departs from Fourth Amendment precepts.

Devin M. Adams *

* J.D. Candidate 2017, University of Richmond School of Law. B.S., 2012, Utah Valley University. I owe a great debt of gratitude to Professor John G. Douglass for his invaluable feedback over the numerous discussions we had throughout the course of this project, and above all, for inspiring me as a writer and advocate. The quality of this piece is especially credited to phenomenal editors, like Katherine Lehnen, and the exemplary members of the *University of Richmond Law Review* who have made this project possible.