Hastings Law Journal

Volume 69 | Issue 5 Article 6

6-2018

The Spider's Parlor: Government Malware on the Dark Web

Kaleigh E. Aucoin

The Spider's Parlor: Government Malware on the Dark Web

Kaleigh E. Aucoin*

The United States government's use of what it refers to as "Network Investigative Tools," presents several constitutional and privacy-related issues. Revelations stemming from the use of these NITs—a form of malware—warrant a difficult discussion on the conflict between public transparency and the level of secrecy required to maintain effective law enforcement. It is especially difficult to focus upon this concern in the context of investigations tackling child pornography, given the unforgiveable nature of crimes against children, and the dire need to apprehend predators. However, the real unease is regarding how online surveillance is conducted, rather than that it is conducted at all. The problem is that unlike certain other forms of technology (for example, phones), there is currently no statutory framework in place to guide law enforcement, the courts, or the public for government hacking. This Note seeks to convey the importance of remaining unblinded by the ends and careful with the means so as not to conflate the significance of the need to capture serious offenders with the justification of ignoring civil liberties.

[*] J.D., University of California, Hastings College of the Law, 2018. I must direct a thousand "thank you"s to Professor Ahmed Ghappour for his indispensable assistance in the creation of this Note, and express endless gratitude to Professor Stefano Moscato for his unparalleled mentorship and guidance throughout my law school career. I also want to thank my teammates on the *Hastings Law Journal* for all their hard work in bringing this Note to print. Last, but never least, I cannot accept any success in my career without acknowledging the love, sacrifice, and support which made it all possible: so, Mom, Dad, this is for you.

TABLE OF CONTENTS

> The Spider turned him round about, and went into his den,
> For well he knew the silly Fly would soon come back again:
> So he wove a subtle web, in a little corner sly,
> And set his table ready, to dine upon the Fly.[1]

INTRODUCTION

Over the last few decades, whispers of an Orwellian surveillance state[2] in the United States have escalated as leaked documents continue

[1] MARY HOWITT, THE SPIDER AND THE FLY (1829). The title of this Note is inspired by this poem as the cautionary tale warns against falling prey to a predator masking his true intentions behind flattery. Here, the masking used by the predator—Tor—is infiltrated by government relying upon that predator's sense of safety behind technology.

[2] *See, e.g.*, Cora Currier et al., *Mass Surveillance in America: A Timeline of Loosening Laws and Practices*, PROPUBLICA (June 7, 2013), https://projects.propublica.org/graphics/surveillance-timeline (providing background on a series of leaks exposing mass surveillance programs run by the National Security Agency).

to expose secret government programs of Big Brother invasions.[3] This information has brought law enforcement activities formerly in the dark into the light of public scrutiny. The fight for privacy is now a race between the government and the individual—one upping the ante through mass invasions of privacy, the other responding with more creative forms of technological concealment.[4] Unsealed court documents reveal, however, a dangerous tool in the government's arsenal: hacking.

This Note describes the development of the Federal Bureau of Investigation's ("FBI") use of Network Investigative Tools ("NITs") in four parts, analyzing the issues surrounding government hacking. First, the Note provides a brief background of privacy in digital spaces. Next, the Note describes the obstacles posed by law enforcement with growing advances in privacy-enhancing technology. Then, the Note details an explanation of hacking generally, followed by a discussion of government hacking specifically with a particular focus on the "Playpen" cases.[5] Finally, the Note analyzes the implications of government hacking and concludes that Congress should enact a comprehensive statute like Title III of the Omnibus Crime Control and Safe Streets Act ("Wire Tap Act" or "Title III")[6] to set clear standards and guidance for law enforcement, thereby legitimatizing its hacking operations and safeguarding individual liberties through oversight.

I. GOVERNMENT SURVEILLANCE: THE GOVERNMENT'S FLYTRAP

A. THE TANGLED WEB WE WEAVE: A PUBLIC SPIDERWEB[7]

The Fourth Amendment states that "[t]he right of the people to be *secure* in their persons, houses, papers, and effects, *against unreasonable searches and seizures*, shall not be violated . . . ."[8] The Supreme Court was clear in *Katz v. United States*—"the Fourth

[3] *See* GEORGE ORWELL, NINETEEN EIGHTY-FOUR 3 (Plume Centennial ed. 1983) (1949) ("You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized.").

[4] *See* Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 19 (2004) ("There has been an ongoing arms race between law enforcement agents who want to use electronic surveillance and those who want to avoid monitoring.").

[5] *See infra* Part IV.

[6] 18 U.S.C. §§ 2510–2522 (2016).

[7] *See* SIR WALTER SCOTT, *Canto Sixth: The Battle*, *in* MARMION: A TALE OF FLODDEN FIELD IN SIX CANTOS, XVII 169 (1892) ("Oh, what a tangled web we weave, [w]hen first we practice [sic] to deceive!"); Paul Gil, *The Difference Between the Internet and the Web*, LIFEWIRE, https://www.lifewire.com/difference-between-the-internet-and-the-web-2483335 (last updated Nov. 2, 2017) (calling the Internet "a public spiderweb of millions of personal, government, educational and commercial computers").

[8] U.S. CONST. amend. IV (emphasis added).

Amendment protects *people*, not places."[9] *Katz* also provided that constitutional protections are afforded to that which one aims to keep private, but clarified that no such protection exists over anything one "knowingly exposes to the public[.]"[10] The result of *Katz* is that, in order to be protected from unreasonable searches, an individual must manifest a subjective expectation of privacy that "society is prepared to recognize as 'reasonable.'"[11] Individuals do not have a reasonable expectation of privacy in information freely provided to third parties.[12] Consequently, any information that one reveals to a third-party service provider to facilitate communications is not protected.[13] In short, just as one assumes the risk of trusting "false" friends with confidential information,[14] one cannot rely upon the privacy of bank records,[15] telephone numbers dialed,[16] Internet Protocol ("IP") addresses,[17] or metadata.[18]

A person's expectations of privacy in the home[19] are complicated by the reality that people do not need to physically leave their four walls to lose the home's traditional protections when entering digital spaces.[20]

[9] 389 U.S. 347, 351 (1967) (emphasis added).

[10] *Id.*

[11] *Id.* at 361 (Harlan, J., concurring).

[12] United States v. Miller, 425 U.S. 435, 443 (1976) (explaining that the Fourth Amendment does not offer protection to "a wrongdoer's misplaced belief that a person to whom he voluntarily confides his wrongdoing will not reveal it") (quoting Hoffa v. United States, 385 U.S. 293, 302 (1966)); United States v. White, 401 U.S. 745, 752 (1971) (providing "one contemplating illegal activities must realize and risk that his companions may be reporting to the police").

[13] OFFICE OF LEGAL EDUC., SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 6 (3d ed. 2009).

[14] *Miller*, 425 U.S. at 443.

[15] *Id.*

[16] Smith v. Maryland, 442 U.S. 735, 742 (1979) ("All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed.").

[17] The Supreme Court has not yet addressed the issue, however, the Third, Fourth, Sixth, Ninth, and Tenth Circuits have all held that that individuals do not have a reasonable expectation of privacy in their IP addresses. United States v. Johnson, No. 15-00340-01-CR-W-GAF, 2016 WL 6136586, at *3 (W.D. Mo. Oct. 20, 2016). *See, e.g.*, United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008) ("[u]sers have no expectation of privacy in the to/from addresses of their messages or [] IP addresses . . . because they should know that this information is provided to and used by Internet service providers for the specific purpose of directing the routing of information.").

[18] "Metadata" refers to "data about data" or "a means by which the complexity of an object is represented in a simpler form." JEFFREY POMERANTZ, METADATA 12 (2015). *Metadata* in an email includes the to/from fields, the IP addresses of the servers handing the email's transition from origin to recipient, and the subject line, whereas the *contents* are the body of the email itself. *Forrester*, 512 F.3d at 510.

[19] *See* Silverman v. United States, 365 U.S. 505, 511 (1961) ("At the very core [of the Fourth Amendment] stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion.").

[20] Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1209–10 (2004).

The Internet is a collection of millions of connected computers and devices throughout the world, which is not owned, controlled, or governed by any single authority.[21] It serves as an incredible tool for communication, dissemination of information, and collaboration across the globe.[22] However, it is easy to forget that every click a user makes corresponds to a log somewhere else.[23] All data that individuals consume—be it images, audio, or time—is broken down into small units of communication which are transmitted through digital networks and then reassembled upon reaching their destination.[24]

One is able to connect to the Internet at home by subscribing to it through third-parties called Internet Service Providers ("ISPs") such as Comcast or AT&T.[25] When a subscriber connects to the Internet, their ISP issues a unique IP address to that subscriber's computer terminal.[26] This identifier consists of a string of numbers and letters used to identify devices and route network traffic on the Internet.[27] IP addresses can be used to identify the subscriber's geographic location, ISP, and the identity of the person who pays for the ISP account.[28] However, obtaining information associated with a given IP address is not as simple as a click.[29] Beyond this, an IP address can change often, and ISPs generally only keep records of IP addresses assigned to a given subscriber for a period between thirty and ninety days,[30] after which time, the IP address

[21] Paul Gil, *Internet 101: Beginners Quick Reference Guide*, LIFEWIRE, https://www.lifewire.com/internet-101-beginners-quick-reference-guide-2483357 (last updated July 19, 2017).

[22] BARRY M. LEINER ET AL., INTERNET SOC'Y, *Brief History of the Internet 1997* 2 (2017) ("The Internet represents one of the most successful examples of the benefits of sustained investment and commitment to research and development of information infrastructure.").

[23] FRANCIS M. ALLEGRA ET AL., PLUGGED IN: GUIDEBOOK TO SOFTWARE AND THE LAW app. 3A (5th ed. 2015).

[24] Nadeem Unuth, *Data Packets: The Building Blocks of Networks*, LIFEWIRE, https://www.lifewire.com/what-is-a-data-packet-3426310 (last updated Feb. 9, 2018).

[25] Paul Gil, *Top 20 Internet Terms for Beginners*, LIFEWIRE, https://www.lifewire.com/top-internet-terms-for-beginners-2483381 (last updated July 30, 2017).

[26] United States v. Christie, 624 F.3d 558, 563 (3d Cir. 2010).

[27] AARON MACKEY ET AL., ELEC. FRONTIER FOUND., UNRELIABLE INFORMANTS: IP ADDRESSES, DIGITAL TIPS AND POLICE RAIDS 5 (2016), https://www.eff.org/files/2016/09/22/2016.09.20_final_formatted_ip_address_white_paper.pdf; Gil, *supra* note 25.

[28] Kevin Mitnick, *Famed Hacker Kevin Mitnick Shows You How to Go Invisible Online*, WIRED (Feb. 24, 2017, 12:00 PM), https://www.wired.com/2017/02/famed-hacker-kevin-mitnick-shows-go-invisible-online/ ("Any communication, whether it's email or not, can be used to identify you based on the [IP] address that's assigned to the router you are using while you are at home, work, or a friend's place.").

[29] *See* MACKEY ET AL., *supra* note 27, at 5–6 ("[T]here is no central map or phonebook that connects IP addresses to particular locations, particularly given that IP addresses are often reassigned to different Internet users over time. . . . [So] unlike street addresses, IP addresses are not static.").

[30] *Christie*, 624 F.3d at 563 (discussing the difficulty posed when known IP address have gone stale due to the time between access to the IPs and subpoenaing ISPs).

may be assigned to someone else.[31] Further, website administrators cannot see the name associated with a given IP address as ISPs hold that information, and generally require subpoenas to disclose it.[32]

It follows that when one visits a website, one leaves a trail behind, as certain information, including one's IP address, is recorded by that website.[33] Today, people consider their computers, phones, and smart tablets, incredibly private, as one is able to instantaneously send exceedingly personal information to anyone from anywhere in the world with a simple click.[34] This convenience continues to change society's understanding of what it means to keep something private.[35] However, people still precariously cling to an illusion of privacy despite the slow erosion of its protections in a digital age.[36] Advances in privacy-enhancing technologies work to guard against the mounting insecurities posed by digital spaces.[37]

B. "GOING DARK": ENCRYPTION AND PEELING BACK LAYERS OF THE ONION ROUTER

Encryption provides one form of security in communication by scrambling one's data so that an intercepting party is unable to decipher

[31] MACKEY ET AL., *supra* note 27, at 5–6.

[32] *See Christie*, 624 F.3d at 562; Joshua J. McIntyre, Comment, *Balancing Expectations of Online Privacy: Why Internet Protocol (IP) Addresses Should Be Protected as Personally Identifiable Information*, 60 DEPAUL L. REV. 895, 897 (2011) ("By comparing its own IP address logs to those maintained by the Internet's Web servers, an ISP can readily link online activity to a specific subscriber account.").

[33] Paul Ohm, *Massive Hard Drives, General Warrants, and the Power of Magistrate Judges*, 97 VA. L. REV. 1, 7 (2011) ("[P]eople produce and retain personalized digital information at a rapidly increasing rate. . . . [O]ur web browsers remember[] every website we visit, stor[e] the addresses in history and copies of the pages themselves in cache."); Bradley Mitchell, *WWW–World Wide Web*, LIFEWIRE, https://www.lifewire.com/history-of-world-wide-web-816583 (last updated Dec. 27, 2017) ("[S]ignificant amounts of personal information including a person's search history and browsing patterns are routinely captured (often for targeted advertising purposes) along with some geolocation information.").

[34] *See* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010).

[35] KEVIN MITNICK, THE ART OF INVISIBILITY 5 (2017) ("Many of us . . . now accept to at least some degree the fact that everything we do—all our phone calls, our texts, our e-mails, our social media—can be seen by others.").

[36] *See* Fred H. Cate, *Government Data Mining: The Need for A Legal Framework*, 43 HARV. C.R.-C.L. L. REV. 435 (2008); Freiwald, *supra* note 4, at 13 ("If we reach a point where we can keep nothing from the government's prying eyes, then we will have lost not only our privacy, but the full exercise of our rights of speech, association, and dissent. In important ways we will have lost our democracy.").

[37] *See* Sam Guiberson et. al., *A Beginner's Guide to Surveillance, Digital Security, and the Privilege*, 40-AUG CHAMPION 52, 55 (2016) ("It is critical to remember that security is a process, not a purchase. No tool is going to give you absolute protection from surveillance in all circumstances.").

it.[38] Though an important tool for secure communications,[39] by all FBI accounts, encryption places the world in jeopardy of "going dark."[40] The concern is that encryption prevents law enforcement from obtaining information, even with a court order, from encrypted devices.[41] Law enforcement maintains that steps must be taken in order to ensure that the government has access to this information; one such suggestion is mandating exceptional access or platform backdoors.[42] However, the call for these type of solutions is controversial because security specialists warn of the inherent risks involved.[43] Furthermore, even if law enforcement is able to decrypt the message sent, it means little if they cannot identify where that message was sent *from*.

Technology which enables additional anonymity is especially problematic for law enforcement because it impedes government's attempts to pinpoint those engaging in nefarious activities online.[44] Enter "Tor," or "The Onion Router," a service comprised of two parts: downloadable software which allows users to access the web with anonymity, and a volunteer network of computers from around the world which enables that software to function.[45] Tor was originally developed for the purpose of guarding government communications in the mid-

[38] This process is accomplished by using algorithms in combination with a piece of secret data called a "key." Nadeem Unuth, *What Is End-to-End Encryption?*, LIFEWIRE, https://www.lifewire.com/what-is-end-to-end-encryption-4028873 (last updated Feb. 23, 2018); Steven M Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 39 n.171 (2014).

[39] *See* Gary C. Kessler, *An Overview of Cryptography*, GARYKESSLER.NET, http://www.garykessler.net/library/crypto.html#purpose (last updated Feb. 22, 2018) ("In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about *any* network, particularly the Internet.").

[40] *See* HAROLD ABELSON ET AL., KEYS UNDER DOORMATS: MANDATING INSECURITY BY REQUIRING GOVERNMENT ACCESS TO ALL DATA AND COMMUNICATIONS (2015); Johnathan Mayer, *Government Hacking*, 127 YALE L.J. 570, 577 (2018) ("One aspect of the [going dark] debate is indisputable: certain law enforcement techniques for electronic searches and seizures are no longer effective, and the natural substitute for those techniques is hacking.").

[41] Editorial Board, Opinion, *Putting the Digital Keys to Unlock Data Out of Reach of Authorities*, WASH. POST (July 18, 2015), https://www.washingtonpost.com/opinions/putting-the-digital-keys-to-unlock-data-out-of-reach-of-authorities/2015/07/18/.

[42] *See* James B. Comey, Dir., Fed. Bureau of Investigation, Remarks at Brookings Institution: Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? (Oct. 16, 2014) (providing that law enforcement suffers from "F.O.M.O." or "fear of missing out" as a result of encryption); KRISTIN FINKLEA, CONG. RESEARCH SERV., ENCRYPTION AND THE "GOING DARK" DEBATE (2016) (summarizing the "going dark" debate).

[43] *See* ABELSON ET AL., *supra* note 40 (discussing the risks of mandated backdoors).

[44] *See Going Dark: Encryption, Technology, and the Balances Between Public Safety and Privacy*, Remarks Before the S. Judiciary Comm. (2015) (joint statement of James B. Comey, Dir., Fed. Bureau of Investigation & Deputy Att'y Gen. Sally Yates, explaining the obstacles posed to law enforcement).

[45] This volunteer network is made up of "relays," "routers," and/or "nodes" which come in three kinds: "middle relays, exit relays, and bridges." *What Is Tor?*, ELEC. FRONTIER FOUND., https://www.eff.org/torchallenge/what-is-tor.html (last visited May 7, 2018).

1990s as a project of the United States Naval Research Laboratory.[46] Currently, Tor is a nonprofit organization and it continues to be funded in part by the government because the United States recognizes its value.[47] Intelligence agencies and law enforcement are said to court "a love-hate relationship with Tor" because although these agencies use Tor, their investigations are hindered when targets use Tor as well.[48]

When most people think of the Internet, they think of the surface web: that is, anything which is indexable by a search engine like Google.[49] But what appears on the surface is just the tip of the proverbial iceberg because most of the Internet "is submerged below."[50] This un-indexable part of the Internet is known as the "deep web" which refers to everything which *cannot* be found via search engines.[51] Within the deep web exists the dark web. The dark web refers to online content which can only be accessed with the use of "specialized encryption software"[52] like that of Tor.[53] On the dark web, there are special websites which end in ".onion" known as "hidden services"[54] with "theoretically untraceable" physical locations.[55] These physical locations are "theoretically untraceable" because the hidden services are masked behind layers of routing like an onion.[56] Despite the legitimate uses of many of these sites,[57] Tor is also

[46] *Users of Tor*, TOR PROJECT, https://www.torproject.org/about/torusers.html.en (last visited May 7, 2018); ONION ROUTING, https://www.onion-router.net/ (last visited May 7, 2018).

[47] *Tor: Myths and Facts*, ELEC. FRONTIER FOUND., https://www.eff.org/document/tor-myths-and-facts (last visited May 7, 2018).

[48] 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/.

[49] *Clearing Up Confusion—Deep Web vs. Dark Web*, BRIGHT PLANET (Mar. 27, 2014), https://brightplanet.com/2014/03/clearing-confusion-deep-web-vs-dark-web/.

[50] THOMAS OLOFSSON, INTELLIAGG, DEEP LIGHT—SHINING A LIGHT ON THE DARK WEB (2016), https://media.scmagazine.com/documents/224/deeplight_(1)_55856.pdf (utilizing the metaphor of a glacier to illustrate the "size discrepancy" between the surface web and the deep web).

[51] TELECOMMUNICATION MARKETS: DRIVERS AND IMPEDIMENTS 143 (Brigitte Preissl et al. eds., 2009).

[52] OLOFSSON, *supra* note 50.

[53] BRIGHT PLANET, *supra* note 49.

[54] Tom Simonite, *"Dark Web" Version of Facebook Shows a New Way to Secure the Web*, M.I.T. TECH REV. (Nov. 3, 2014), https://www.technologyreview.com/s/532256/dark-web-version-of-facebook-shows-a-new-way-to-secure-the-web/.

[55] Poulsen, *supra* note 48; *see* Jesse Atlas, Opinion, *Insider Trading on the Dark Web*, FORBES (Mar. 25, 2014, 8:00 AM), https://www.forbes.com/sites/realspin/2014/03/25/insider-trading-on-the-dark-web/#1e3674d46a61 ("Without an IP address, it is nearly impossible to trace users back to their computers. Thousands of people evaded the FBI by using the Tor browser to do illicit deals on sites like The Silk Road—the e-bay for drugs, guns, and hit men.").

[56] Poulsen, *supra* note 48.

[57] *See, e.g.*, Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1087 (2017) (discussing how Tor provides protection from two different types of surveillance: traffic analysis and acquisition of metadata); Mike Tigas, *A More Secure and Anonymous ProPublica Using Tor Hidden Services*, PROPUBLICA (Jan. 13, 2016, 10:45 AM), https://www.propublica.org/nerds/a-more-secure-and-anonymous-propublica-using-tor-hidden-services (providing that a hidden service version of the site was launched to protect readers from

brimming with illicit activities.[58] More troubling is that the dark web acts like a nefarious whack-a-mole, so that once one elicit enterprise is taken offline, another pops up in its place.[59] Just as people with legitimate purposes,[60] those who use Tor for reprehensible purposes do so with complete anonymity[61] so the government has had to get creative in its tactics.

II. GOVERNMENT HACKING

A. KNOWN FBI OPERATIONS

"Hacking" refers to the manipulation and bypassing of systems to force those systems to do something unintended.[62] While the act of hacking historically did not denote the manipulation of computer systems, today, the term usually pertains to "any technical effort to manipulate the normal behavior of network connections and connected systems."[63] "Hacker" is not an inherently criminal term and generally, hackers come in three flavors: white hats, gray hats, and black hats.[64] One of the ways that hackers execute criminal schemes is through the use of malware—short hand for "malicious software"—which refers to any kind of software that is explicitly intended to obtain access to one's computer

surveillance because "[o]ur readers should never need to worry that somebody else is watching what they're doing on our site"); David Talbot, *Dissent Made Safer*, M.I.T. TECH. REV. (Apr. 21, 2009), https://www.technologyreview.com/s/413091/dissent-made-safer/ (discussing how Tor is enabled to circumvent government censorship and surveillance).

[58] *See, e.g.*, *Buying Drugs Online: Shedding Light on the Dark Web*, ECONOMIST (July 16, 2016), https://www.economist.com/news/international/21702176-drug-trade-moving-street-online-cryptomarkets-forced-compete (providing an in-depth study of drugs on the dark web).

[59] *See* Steven Nelson, *Buying Drugs Online Remains Easy, 2 Years After FBI Killed Silk Road*, U.S. NEWS (Oct. 2, 2015, 3:12 PM), https://www.usnews.com/news/articles/2015/10/02/buying-drugs-online-remains-easy-2-years-after-fbi-killed-silk-road ("[M]ore than half of anonymous marketplaces implement websites that are directly derived from them template the Silk Road used, and from formatting all the way to policy Silk Road invented the status quo that actors in this space have come to expect[].").

[60] The anonymity offered by Tor is important as attorneys, corporations, journalists, and governments all use Tor. *See* Brief of Amicus Curiae Elec. Frontier Found., at 3, U.S. v. Matish, No. 4:16-cr-16 (E.D.Va. May 9, 2016); Simonite, *supra* note 54 ("Tor users include dissidents trying to avoid censorship, criminals, and U.S. government workers who need to escape scrutiny from foreign scrutiny services.").

[61] *See* Guiberson et al., *supra* note 37.

[62] *See* Paul Gil, *The Greatest Computer Hacks*, LIFEWIRE, https://www.lifewire.com/the-greatest-computer-hacks-4060530 (last updated Sept. 19, 2017).

[63] Bradley Mitchell, *What Is Hacking?*, LIFEWIRE, https://www.lifewire.com/definition-of-hacking-817991 (last updated Mar. 12, 2018).

[64] For a discussion on the distinction, see Kim Zetter, *Hacker Lexicon: What Are White Hat, Gray Hat, and Black Hat Hackers?*, WIRED (Apr. 13, 2016, 5:03 PM), https://www.wired.com/2016/04/hacker-lexicon-white-hat-gray-hat-black-hat-hackers/.

without computer the owner's consent.[65] Malware comes in many forms, including: spyware,[66] ransomware,[67] keyloggers,[68] viruses,[69] "or any type of malicious code that infiltrates a computer."[70] When any form of malware goes unfixed, or without a "patch" it is referred to as "in the wild."[71] As long as malware remains in the wild, people stay vulnerable to attack until an antidote, or a "patch" is created.

The FBI has used a wide variety of terminology to refer to its own hacking operations,[72] opposed to associations with malware and hacking because both activities suggest that the activity is unlawful.[73] To this end, the government has maintained that its operations are court sanctioned and therefore different.[74] However, a Network Investigative Technique ("NIT"), by practical definition, is a form of malware because it is designed to gain access to one's computer without one's consent to do so. Semantics aside, the government is able to surreptitiously infiltrate one's computer remotely, frequently without adequate oversight from the courts.[75] It is estimated that the FBI has used malware for almost two decades[76] but the way the malware is deployed has changed over time as a result of Tor and other technology designed to mask one's identity and location online.[77]

[65] *The Playpen Cases: Frequently Asked Questions*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/playpen-cases-frequently-asked-questions (last visited May 7, 2018).

[66] Spyware is surreptitiously installed onto a victim's device to collect that victim's information. *See* Tim Fisher, *What Is Malware?*, LIFEWIRE, https://www.lifewire.com/what-is-malware-153600 (last updated Jan. 16, 2018).

[67] Ransomware locks a victim's device and prevents access to one's data or threatens to delete or release that data unless a ransom is paid. *See Hacker Lexicon: A Guide to Ransomware, the Scary Hack That's on the Rise*, WIRED (Feb. 9, 2016, 6:00 AM), https://www.wired.com/video/hacker-lexicon-a-guide-to-ransomware-the-scary-hack-that-s-on-the-rise.

[68] A keylogger is malware clandestinely installed onto one's device to monitor and log one's keystrokes then send that information to the attacker. *See* Mary Landesman, *Examples of the Most Damaging Malware*, LIFEWIRE, https://www.lifewire.com/most-damaging-malware-153602 (last updated June 2, 2017).

[69] Computer viruses are programs that, not unlike regular viruses, spread from computer to computer. *See* Anne W. Branscomb, *Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime*, 16 RUTGERS COMPUTER & TECH. L.J. 1, 60 (1990).

[70] *The Playpen Cases: Frequently Asked Questions*, *supra* note 65.

[71] Fisher, *supra* note 66.

[72] For a list of these terms, see Mayer, *supra* note 40, at 575 n.16.

[73] Mayer, *supra* note 40, at 575 n.16 (explaining the government's opposition to NITs' associations with malware or hacking).

[74] Decl. of Dr. Christopher Soghoian, United States v. Matish, No. 4:16-cr-00016, at 3 n.9 (E.D. Va. June 10, 2016).

[75] *Government Hacking and Subversion of Digital Security*, ELEC. FRONTIER FOUND., https://www.eff.org/issues/government-hacking-digital-security (last visited May 7, 2018).

[76] Andrew Crocker, *With Remote Hacking, the Government's Particularity Problem Isn't Going Away*, JUST SECURITY (June 2, 2016), https://www.justsecurity.org/31365/remote-hacking-governments-particularity-problem-isnt/.

[77] Poulsen, *supra* note 48.

B. THE EARLY DAYS: CARNIVORE, KLS, AND MAGIC LANTERN

Since at least the 1990s, the United States has used computer surveillance tools in its investigations. The first known tool used by the FBI was a "network sniffer"[78] and diagnostic tool dubbed "Carnivore."[79] With the permission of ISPs, the government installed Carnivore onto "network backbones"[80] to target individuals and collect data authorized by wiretap orders.[81] The hardware component which operated the Carnivore system required physical installation at the ISP of that targeted individual.[82] The public did not learn about Carnivore until 2000 when Earthlink, an ISP, refused to allow the FBI to install it on its network.[83] The FBI has since discontinued its use of Carnivore in favor of commercial products.[84]

In 1999, the FBI worked around the problems imposed by encryption by using a keylogger program[85] called the Keystroke Logger System ("KLS") to capture a password.[86] The KLS recorded and monitored all keystrokes entered onto a computer so long as the computer's modem was not in use.[87] Pursuant to two warrants, the FBI physically installed KLS multiple times onto the computer of mobster Nicodemo S. Scarfo.[88] The KLS was apparently necessary to the success of the government's investigation into Scarfo because of Scarfo used

[78] A network sniffer works by monitoring data transmitted over a computer network in real time. *See* Bradley Mitchell, *What Is a Network Sniffer?*, LIFEWIRE, https://www.lifewire.com/definition-of-sniffer-817996 (last updated Aug. 24, 2017).

[79] Kim Zetter, *Everything We Know About How the FBI Hacks People*, WIRED (May 15, 2016, 7:00 AM), https://www.wired.com/2016/05/history-fbis-hacking/.

[80] Network backbones are utilized to enable network traffic and "consist of network routers and switches connected mainly by fiber optic cables" used by ISPs and large organizations. Bradley Mitchell, *What Internet and Network Backbones Do*, LIFEWIRE, https://www.lifewire.com/definition-of-backbone-817777 (last visited May 7, 2018).

[81] Nathan E. Carrell, *Spying on the Mob:* United States v. Scarfo*—A Constitutional Analysis*, 2002 U. ILL. J.L. TECH. & POL'Y 193, 197 (2002).

[82] Brent Dean, *Carnivores and Magic Lanterns: The New World of Electronic Surveillance*, 3 COMPUTER CRIME & TECH. LAW ENFORCEMENT 4 (2007).

[83] Zetter, *supra* note 79 ("Earthlink feared the sniffer would give the feds unfettered access to all customer communications. A court battle and congressional hearing ensued, which sparked a fierce and divisive debate, making Carnivore the Apple/FBI case of its day.").

[84] *See* Zetter, *supra* note 79.

[85] For a description of keyloggers, see Landesman, *supra* note 68.

[86] Declan McCullagh, *How Far Can FBI Spying Go?*, WIRED (July 31, 2001, 12:00 PM), https://www.wired.com/2001/07/how-far-can-fbi-spying-go/.

[87] *See* United States v. Scarfo, 180 F. Supp. 2d 572, 581–82 (D.N.J. 2001). By only recording when the modem was not in use, the FBI avoided triggering Title III protections as Title III warrants are only required when capturing statutorily defined oral, electronic, or wire communications. *See* Carrell, *supra* note 81, at 198.

[88] *See Scarfo*, 180 F. Supp. 2d. at 574 ("This case presents an interesting issue of first impression dealing with the ever-present tension between individual privacy and liberty rights and law enforcement's use of new and advanced technology to vigorously investigate criminal activity.").

Pretty Good Privacy ("PGP")[89] software to encrypt a file on his computer entitled "Factors."[90] The FBI obtained a warrant in order to obtain the password to decrypt the software and access the file, believing the file contained information pertaining to Scarfo's illegal gambling and loansharking operation.[91]

Scarfo's defense made several points in its arguments to suppress evidence obtained through the KLS—namely that the warrant was void as a general warrant;[92] and the installation of the KLS amounted to a wiretap subject to Title III protections.[93] The court rejected both arguments.[94] Scarfo's defense became more complicated when he pursued information about the keylogger.[95] The government filed a motion under the Classified Information Procedures Act ("CIPA"), insisting that the technology at issue "was classified for national security reasons."[96] Along with other things, CIPA allows for the government to redact certain information and provide non-classified summaries in its place as a part of discovery.[97] This move was successful for the government, and the KLS was never disclosed.[98]

In 2001, it came to light that the FBI developed a software version of KLS named "Magic Lantern."[99] Unlike its predecessor, Magic Lantern could be remotely installed via a computer virus.[100] This remote access search technique[101] had the ability to record keystrokes in addition to emailing data back to law enforcement.[102] Magic Lantern is believed to

[89] PGP is encryption software created by Philip Zimmerman in the 1990s utilizing a two-key system which requires a passphrase to encrypt and a passphrase to decrypt. Carrell, *supra* note 81, at 193, 196; *see* Kessler, *supra* note 39 (explaining the process of using PGP).

[90] *See Scarfo*, 180 F. Supp. 2d. at 574, 581.

[91] *Id.*

[92] *See* Declan McCullagh, *Feds Use Keylogger to Thwart PGP, Hushmail*, CNET (July 20, 2007, 10:41 AM), https://www.cnet.com/news/feds-use-keylogger-to-thwart-pgp-hushmail/.

[93] *See Scarfo*, 180 F. Supp. 2d at 576; SAYAKO QUINLAN & ANDI WILSON, A BRIEF HISTORY OF LAW ENFORCEMENT HACKING IN THE UNITED STATES 3 (2016) ("[I]n a two-year pretrial court fight, Scarfo challenged the legality of using the key logging software, claiming that the tool was akin to wiretapping and that the FBI had not obtained the proper warrant for its use.").

[94] *See Scarfo*, 180 F. Supp. 2d at 576, 581.

[95] Zetter, *supra* note 79.

[96] Zetter, *supra* note 79 ("[I]t's one of the same excuses the government uses today to keep a veil over its surveillance tools and techniques").

[97] *See Scarfo*, 180 F. Supp. 2d at 579.

[98] *Id.* at 583 ("CIPA strikes a balance between national security interests and a criminal defendant's right to discovery by allowing for a summary which meets the defendant's discovery needs.").

[99] Zetter, *supra* note 79 ("The Scarfo case evidently convinced the feds that they needed to develop their own custom hacking tools . . . .").

[100] Carrell, *supra* note 81, at 198, 199.

[101] *See* Zach Lerner, *A Warrant to Hack: An Analysis of the Proposed Amendments to Rule 41 of the Federal Rules of Criminal Procedure*, 18 YALE J. L. & TECH. 26, 39–40 (2016) (explaining how remote access tools work).

[102] Carrell, *supra* note 81, at 199.

be the software used in the first known instance of the government hacking *remotely*, taking place in early 2003.[103] The FBI's investigation into six animal activists—called "Operation Trail Mix"—centered upon the actions of the U.S.-based branch of an organization dedicated to shutting down Huntingdon Life Sciences, a research firm that utilized animal product testing.[104] Again, the FBI found itself thwarted by the group's use of PGP software in masking its online communications and attempted to get around the encryption by obtaining a wiretap order to intercept the group's computers.[105]

C. PHISHING, AND WATERING HOLE ATTACKS

In 2007, Timberline High School of Lacey, Washington, was subject to nine bomb threats[106] sent from an anonymous source—via a handwritten note, emails, and through a Myspace page called "Timberlinebombinfo."[107] The FBI turned to Google and Myspace to track down the hoaxer, however, the culprit masked his identity so that it appeared the threats were coming from Italy or the Czech Republic.[108] Because of these threats, and the wrongdoer's use of anonymizing software, the FBI filed for authorization of a search warrant to install malware called Computer and Internet Protocol Address Verifier ("CIPAV") onto any device accessing the Timberlinebombinfo Myspace account.[109] The FBI used a popular form of hacking known as "phishing"[110] which entails impersonating a non-threatening and trustworthy website or the like then tempting a victim to click on a link

[103] Matt Apuzzo, *F.B.I. Used Hacking Software Decade Before iPhone Fight*, N.Y. TIMES (Apr. 13, 2016), http://www.nytimes.com/2016/04/14/technology/fbi-tried-to-defeat-encryption-10-years-ago-files-show.html?_r=0.

[104] *See* United States v. Fullmer, 584 F.3d 132, 138 (3d Cir. 2009); Zetter, *supra* note 69.

[105] Apuzzo, *supra* note 103.

[106] *See* Mayer, *supra* note 40, at 574; Raphael Satter, *How a School Bomb-Scare Case Sparked a Media-vs.-FBI Fight*, U.S. NEWS (Mar. 18, 2017, 3:03 AM), https://www.usnews.com/news/best-states/washington/articles/2017-03-18/how-a-school-bomb-scare-case-sparked-a-media-vs-fbi-fight ("Each time a threat came in, the school would be emptied. Each time, nothing happened.").

[107] *See* Brian L. Owsley, *Beware of Government Agents Bearing Trojan Horses*, 48 AKRON L. REV. 315, 324–27 (2015) (describing the events of the Timberline High School bomb threats in detail).

[108] Satter, *supra* note 106 ("The hacker had broken into the servers and used them to throw investigators off. He could have been hiding anywhere . . . [the hacker, 15 years old at the time] relied largely on two or three servers that he had penetrated from his home computer. He typically emailed his threats between the time his parents left for work and when he took the bus to school.").

[109] Owsley, *supra* note 107, at 316, 325.

[110] *See* Kim Zetter, *Hacker Lexicon: What Is Phishing?*, WIRED (Apr. 7, 2015, 6:09 PM), https://www.wired.com/2015/04/hacker-lexicon-spear-phishing/:

> Phishing refers to malicious emails that are designed to trick the recipient into clicking on a malicious attachment or visiting a malicious web site. Spear-phishing is a more targeted form of phishing that appears to come from a trusted acquaintance . . . An estimated 91-percent of hacking attacks begin with a phishing or spear-phishing email.

or a document which then infiltrates the victim's computer with malware.[111] Banking on the conceit of the hoaxer, an FBI agent messaged the Myspace account pretending to be a reporter sending links to an article he was compiling.[112] When the suspect clicked on the link, CIPAV ran on his computer, relaying his IP address back to the FBI.[113] Once the FBI obtained the IP address, agents could subpoena the ISP for the subscriber's information.[114] From there, the FBI was able to secure the identity of the teen behind the threats and quickly arrested him hours after he clicked on the malicious link.[115]

Another law enforcement hacking technique is the "watering hole attack,"[116] also known as a "drive-by-download," which works so that anyone who visits a website infected with malware is then infected.[117] This tool is ideal in situations where the hidden services on the dark web contain contraband, like that of child pornography, which is illegal to seek out or view. There are three known federal investigations to date that used this watering hole attack on the dark web: (1) "Operation Torpedo" in 2012; (2) the take down of Freedom Hosting servers in 2013; and (3) "Operation Pacifier" in 2015.[118] It is estimated that these investigations resulted in a collective hacking of thousands of computers from around the world.[119]

The first time the FBI has had to publicly defend its watering hole tactic was with "Operation Torpedo."[120] In Operation Torpedo,

[111] Jenna McLaughlin, *The Big Secret That Makes the FBI's Anti-Encryption Campaign a Big Lie*, INTERCEPT (Sept. 28, 2015, 7:47 AM), https://theintercept.com/2015/09/28/hacking/.

[112] *See* Satter, *supra* note 106 (detailing the use of the AP website and FBI agent pretending to be a reporter to catch the person behind the Timberline High school bomb threats).

[113] Satter, *supra* note 106.

[114] Lerner, *supra* note 101, at 39.

[115] McLaughlin, *supra* note 111. Two days after the culprit's sentencing, *Wired* broke the story that the FBI used the CIPAV software. *See* Kevin Poulsen, *FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats*, WIRED (July 8, 2007, 12:00 PM), https://www.wired.com/2007/07/fbi-spyware/. From there, the Electronic Frontier Foundation filed a Freedom of Information Act request to access all documents pertaining to the program. *See Endpoint Surveillance Tools (CIPAV)*, ELEC. FRONTIER FOUND., https://www.eff.org/foia/foia-endpoint-surveillance-tools-cipav (last visited May 7, 2018). While the documents received were heavily redacted, the EFF had enough to determine the variety of information that was collected from a target's computer once the CIPAV is installed onto it, and to determine that the FBI "and likely other federal agencies—have used this tool a lot." Jennifer Lynch, *New FBI Documents Provide Details on Government's Surveillance Spyware*, ELEC. FRONTIER FOUND.: DEEPLINKS BLOG (Apr. 29, 2011), https://www.eff.org/deeplinks/2011/04/new-fbi-documents-show-depth-government.

[116] "The term derives from the concept of poisoning a watering hole where certain animals are known to drink." AM. C.L. UNION FOUND. ET AL., CHALLENGING GOVERNMENT HACKING IN CRIMINAL CASES 1 (2017).

[117] McLaughlin, *supra* note 111.

[118] *See* Mayer, *supra* note 40, at 584–85.

[119] Mayer, *supra* note 40, at 585.

[120] Poulsen, *supra* note 48.

authorities in the Netherlands benefited from the lack of precaution of the administrator of a hidden service called "Pedo Board."[121] This individual left his administrative account open without a password so the agents were able to access the account and trace the server's IP address to Nebraska.[122] They then passed the information along to the FBI.[123] The FBI traced the IP address to Aaron McGrath, who operated three servers hosting child pornography.[124] The FBI spent a year investigating McGrath until finally arresting him and seizing his servers.[125] A federal magistrate issued three search warrants sanctioning the FBI to install malware onto the hidden service and deploy NITs on any computers which visited it.[126] The FBI deployed the NIT by utilizing a vulnerability in the Adobe Flash Player plugin for the Tor Browser.[127] The NIT was only authorized to collect specific information on these computers.[128] Once the IP addresses of these computers were identified, the law enforcement subpoenaed the ISPs to obtain the subscriber's names and home addresses, and used this information to apply for further search warrants then execute cross-country arrests.[129]

In 2013, the government performed another take down of child pornography on the dark web with an unnamed operation against "Freedom Hosting" servers, a large and unidentified provider hosting Tor hidden services—many of which were contraband.[130] Eric Eoin Marques—an American born Irishman—was living in Dublin, Ireland in July 2013 when he was arrested by Irish authorities.[131] Marques, in running the Freedom Hosting servers, is believed to be the biggest

[121] Poulsen, *supra* note 48.

[122] Poulsen, *supra* note 48.

[123] Poulsen, *supra* note 48.

[124] Poulsen, *supra* note 48.

[125] Poulsen, *supra* note 48.

[126] Poulsen, *supra* note 48.

[127] *See* Response & Request to Strike Defendant's Request for Daubert Motion, U.S. v. Cottom, No. 8:13-cr-00108-JFB-TDT, at 5 (D. Neb. June 29, 2015):

> [T]he [NIT] utilized a Flash application that, when downloaded by a user and activated by their browser, made a direct TCP connection to a server that the FBI controlled. Depending on the operating system and version of the user's browser, the connection would bypass the browser's configured proxy server and reveal the user's true IP address.

[128] Poulsen, *supra* note 48.

[129] Poulsen, *supra* note 48.

[130] Poulsen, *supra* note 48 (Freedom Hosting is said to have, "by some estimates, powered half of the Dark Net.").

[131] The U.S. was granted its request for extradition of Eric Eoin Marques in December 2015. *High Court Grants Extradition of Irishman to US in Porn Case*, RAIDIÓ TEILIFÍS ÉIREANN (Dec. 15, 2015, 4:50 PM), https://www.rte.ie/news/ireland/2015/1216/754065-eric-eoin-marques/. Marques appeal of the extradition order was denied in December, 2016. *Man Loses Extradition Challenge in Child Abuse Images Case*, RAIDIÓ TEILIFÍS ÉIREANN (Dec. 12, 2016, 5:37 PM), https://www.rte.ie/news/2016/1212/838362-eric-eoin-marques/.

facilitator of child pornography in the world, who earned thousands of dollars on a monthly basis for his facilitation.[132] The FBI worked with French authorities to gain control over Freedom Hosting servers located in France and was able to relocate these servers to Maryland by cloning them.[133] Shortly thereafter, some Tor users noticed that sites on Freedom Hosting's servers "were serving a hidden 'iframe'—a kind of website within a website."[134] As it turns out, this iframe housed malicious code which used a vulnerability in the Tor browser through Mozilla Firefox to deploy malware.[135] This code specifically targeted the first Tor browser exploit found in the wild in order to gather the target computer's IP address, media access control ("MAC") address, and computer's host name.[136] The code enabled a program on one's computer which invalidated the anonymity offered by the Tor browser.[137] In the process of attempting to apprehend those accessing illegal contraband, the government's code is believed to have indiscriminately attacked potentially innocent users of an email service known as TorMail.[138] The FBI failed to inform any of the users on TorMail—whose identities the FBI never subpoenaed—that their computers were compromised by the attack.[139] This resulted in vulnerability to anyone who had not yet updated their Tor browser bundle with the latest patch. It also leaves unresolved questions as to whether the FBI *should* or is *required* to inform people in similar situations if their computers are compromised by the government without probable cause for criminal activity.

III. OPERATION PACIFICER: THE "PLAYPEN" CASES

A. THE WARRANT DEPLOYED AROUND THE WORLD

In early 2015, the FBI seized the server of a child pornography hidden service known as "Playpen."[140] The FBI became aware of Playpen

[132] *See* Graham Templeton, *The US Is Trying to Extradite a Notorious Dark Web Admin This Week*, VICE: MOTHERBOARD (May 11, 2015, 7:45 AM), https://motherboard.vice.com/en_us/article/the-us-is-trying-to-extradite-a-notorious-dark-web-admin-this-week; IrishCentral Staff Writers, *FBI Most Wanted Pornographer Eric Eoin Marques Lived a Quiet Life*, IRISHCENTRAL (Aug. 26, 2013, 5:12 AM), https://www.irishcentral.com/news/fbi-most-wanted-pornographer-eric-eoin-marques-lived-a-quiet-life-221143181-237772251.

[133] Poulsen, *supra* note 48.

[134] Poulsen, *supra* note 48.

[135] Poulsen, *supra* note 48.

[136] Poulsen, *supra* note 48.

[137] Poulsen, *supra* note 48.

[138] McLaughlin, *supra* note 111.

[139] McLaughlin, *supra* note 111.

[140] *See* Press Release, Dep't of Justice, Florida Man Convicted of Engaging in Child Exploitation Enterprise (Sept. 16, 2016), https://www.justice.gov/opa/pr/florida-man-convicted-engaging-child-exploitation-enterprise.

in December 2014 when it received a tip from a foreign agency that the temporarily visible IP address of the server was in the U.S.[141] The FBI then investigated and obtained a search warrant for the home of the person associated with that IP address and seized the server hosting Playpen.[142] The catalyst of the operation—dubbed "Operation Pacifier"—began when the FBI arrested Stephen Chase, the creator and co-administer of Playpen, and seized his server from his home in Florida.[143] Controversially, instead of shutting Playpen down, the FBI obtained a warrant and ran the site from their servers in Virginia for almost two weeks after apprehending Chase.[144] While this was not the first time the FBI seized then ran websites hosting child pornography, it marked the public's first time knowing about it.[145]

Operation Pacifier also attracted more controversy than its predecessors because a single warrant led to an estimated collection of IP addresses ranging somewhere in the thousands,[146] at least 350 domestic arrests, and over 135 cases nationwide ("Playpen cases").[147] In February 2015, U.S. Magistrate Judge Theresa Carroll Buchanan of the Eastern District of Virginia, issued a search warrant ("NIT Warrant") which authorized the FBI to deploy a NIT on *any* person's computer who logged into Playpen regardless of *where* they logged in from.[148] The NIT Warrant enabled the FBI to hack over 8000 computers[149] and authorized

[141] *The Playpen Cases: Frequently Asked Questions*, *supra* note 65.

[142] *The Playpen Cases: Frequently Asked Questions*, *supra* note 65.

[143] In May 2017, Chase was sentenced to thirty years in federal prison for his horrific crimes. *'Playpen' Creator Sentenced to 30 Years*, FBI NEWS (May 5, 2017), https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years.

[144] *See* Press Release, Dep't of Justice, Barre Resident Sentenced to Prison for Possession of Child Pornography (Oct. 16, 2017) ("The FBI did not shut down the Website for approximately 13 days.").

[145] When the warrant application was unsealed, it was unearthed that the FBI requested authorization to run all twenty-three of elicit hidden service websites hosted by Freedom Hosting from a government facility in Maryland for thirty days. *See* Affidavit ISO Application for Search Warrant, In the Matter of the Search of Computers that Access "Websites 1-23", No. 13-17440 (D. Md. Oct. 13, 2016).

[146] *See* Bellovin, *supra* note 38, at n.152.

[147] *See* Press Release, Dep't of Justice, Shelby County Man Sentenced for Possessing Child Pornography (Dec. 18, 2017), https://www.justice.gov/usao-sdoh/pr/shelby-county-man-sentenced-possessing-child-pornography ("As a result of the investigation, at least 350 U.S.-based individuals have been arrested, 25 producers of child pornography have been prosecuted, 51 alleged hands-on abusers have been prosecuted and 55 American children who were subjected to sexual abuse have been successfully identified or rescued.").

[148] In the Matter of the Search of Computers that Access upf45jvbziuctml.onion, No. 1:15-SW-89 (E.D. Va Feb. 20, 2015) [hereinafter NIT Warrant].

[149] *See* Joseph Cox, *The FBI Hacked over 8,000 Computers in 120 Countries Based on One Warrant*, VICE: MOTHERBOARD (Nov. 22, 2016, 3:18 PM), https://motherboard.vice.com/en_us/article/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant; Joseph Cox, *Court Docs Confirm FBI's Child Porn Hack Was International*, VICE: MOTHERBOARD (May 17, 2016, 3:00 AM), https://motherboard.vice.com/en_us/article/court-docs-confirm-fbis-child-porn-

the FBI to deploy a NIT on the server operating Playpen in order to obtain information from anyone who accessed the hidden service.[150] In each Playpen case, the FBI used the information obtained from the NIT to obtain—among other things—the Tor user's masked IP address.[151] The FBI then used the captured IP address to obtain a subpoena from the associated ISP.[152] Finally, the identifying information from the subpoena, NIT, and the evidence collected from investigations into the user associated with the IP address was used to obtain a residential warrant from the appropriate judicial district to search the home of the defendant.[153]

The FBI refers to this investigation as the FBI's most fruitful operation against criminal activity on the dark web to date.[154] As of February 1, 2018, there are over 200 cases in the United States resulting from the NIT Warrant.[155] Of information available, a total of forty-six U.S. defendants have either pleaded guilty or have been found guilty for various federal charges under the Child Protection Act.[156] Of the at least seventy attorneys, and some thirty legal teams across the country known to be working on the Playpen cases, some have chosen to combine their efforts in a "national working group."[157] A minority of four cases were

hack-was-international ("According to a Europol presentation, the agency has generated 3,229 cases as part of the operation covering Playpen.").

[150] *The Playpen Cases: Frequently Asked Questions*, *supra* note 65.

[151] Specifically, the NIT Warrant authorized the collection of the target computer's host name, operating system, IP address, MAC address, as well as other information. *See* NIT Warrant, *supra* note 148, at 6–7. For an explanation on how the NIT itself worked, see Susan Hennessey & Nicholas Weaver, *A Judicial Framework for Evaluating Network Investigative Techniques*, LAWFARE BLOG (July 28, 2016, 10:17 AM), https://www.lawfareblog.com/judicial-framework-evaluating-network-investigative-techniques (explaining how the "distinct components" of "generator," "exploit," "payload," and "logging server" worked to circumvent the anonymity afforded by Tor).

[152] *See, e.g.*, United States v. Sullivan, 229 F. Supp. 3d 647, 650–51 (N.D. Ohio 2017) (describing the subpoena process in the Playpen cases).

[153] *See The Playpen Cases: Frequently Asked Questions*, *supra* note 65 ("Once the FBI obtained an IP address from the NIT's transmissions, it served subpoenas on [ISPs] to learn the names and addresses associated with that IP address. The FBI then obtained warrants to search and seize evidence associated with child pornography at those locations.").

[154] *See Playpen Creator Sentenced to 30 Years*, *supra* note 143.

[155] *See* Leslie R. Caldwell, *Ensuring Tech-Savvy Criminals Do Not Have Immunity from Investigation*, DEP'T OF JUSTICE (Nov. 21, 2016), https://www.justice.gov/archives/opa/blog/ensuring-tech-savvy-criminals-do-not-have-immunity-investigation.

[156] This number is based on a search of federal dockets on Bloomberg Law as of February 1, 2018. *See, e.g.*, United States v. Duncan, No. 3:15-cr-00414 (D. Or. filed Nov. 19, 2015) (sentenced to twenty-five years in prison followed by supervised release for life), Dkt. Nos. 76, 88; United States v. Henderson, No. 3:15-cr-00565 (N.D. Cal. filed Sept. 1, 2016) (sentenced to five years in prison followed by ten years of supervised release), Dkt. Nos. 70, 83.

[157] *See* Joseph Cox, *Dozens of Lawyers Across the US Fight the FBI's Mass Hacking Campaign*, VICE: MOTHERBOARD (July 27, 2016, 9:15 AM), https://motherboard.vice.com/en_us/article/dozens-of-lawyers-across-the-us-fight-the-fbis-mass-hacking-campaign-playpen ("The group . . . has a Dropbox-like system for sharing material, and a lively Google discussion group. They inform each other of developments, exchange legal documents, and basically help each other out with

dismissed by three district courts following grants of suppression motions, but each decision has since been reversed on appeal by the First, Eighth, and Tenth Circuits.[158] Additionally, the Fourth Circuit affirmed the denial of suppression in a defendant's appeal.[159] At least four cases were dismissed by motion of the government because of discovery orders unfavorable to the government, unclear reasons, or as a result of deaths of defendants.[160]

To date, the Playpen defendants and government prosecution teams have adopted similar arguments and counter arguments regarding the validity of the NIT Warrant and all the information subsequently gathered as a result of its authorization.[161] The Playpen defendants have argued motions for dismissal of their indictments based on "outrageous government conduct;" motions to suppress all evidence based on unconstitutionality and insufficiency of the NIT Warrant; and motions to compel discovery of the source code deployed by the NIT.[162]

B. GOING THROUGH THE MOTIONS: DISMISSAL, SUPPRESSION, AND DISCLOSURE

1. *Motions to Dismiss for Outrageous Government Conduct*

Some of the Playpen defendants called for dismissal of their indictments based on the argument that the FBI's conduct, in hosting

their cases."). The ACLU Foundation, EFF, and National Association of Criminal Defense Lawyers collaborated to create a resource detailing legal strategies for defense attorneys to utilize to even the playing field against the government in hacking cases. *See* Lerner, *supra* note 101.

[158] *See* United States v. Levin, No. 15-CR-10271, 2016 WL 2596010 (D. Mass. May 5, 2016), *rev'd*, 874 F.3d 316 (1st Cir. 2017); United States v. Workman, 205 F. Supp. 3d 1256, 1269 (D. Colo. 2016), *rev'd*, 863 F.3d 1313 (10th Cir. 2017); United States v. Croghan (and Horton), Nos. 15-CR-48, 15-CR-51, 2016 WL 4992105 (S.D. Iowa Sept. 19, 2016), *rev'd*, United States v. Horton, 863 F.3d 1041 (8th Cir. 2017). Some of these defendants have filed for writs of certiorari before the Supreme Court. *See* Horton v. United States, No. 17-6910 (U.S. Nov. 28, 2017); Workman v. United States, No. 17-7042 (U.S. Dec. 12, 2017).

[159] *See, e.g.*, United States v. McLamb, No. 17-4299, 2018 WL 541851, at *3–4 (4th Cir. 2018) (agreeing with the findings of its "sister circuits" that suppression is not an appropriate remedy).

[160] *See* United States v. Michaud, No. 3:15-cr-05351-RJB (W.D. Wash. filed July 23, 2015), Dkt. No. 227 (dismissed after a lengthy discovery battle resulted in a choice between disclosure of the NIT's source code or dropping the case); United States v. Dzwonczyk, No. 4:15-cr-03134 (D. Neb. filed Jan. 3, 2017), Dkt. No. 78 (dismissed following defendant's death); United States v. Kneitel, No. 8:16-cr-00023 (M.D. Fla. filed Jan. 14, 2016), Dkt. Nos. 201–202 (dismissed following guilty verdict after defendant's death); United States v. Arterbury, No. 4:15-cr-00182 (N.D. Okla. filed Nov. 10, 2016), Dkt. No. 67 (dismissed for unclear reasons).

[161] Cox, *supra* note 157 (summarizing the two chief defense strategies adopted nationwide: (1) suppression of evidence from the NIT Warrant, and (2) disclosure of the full NIT source code).

[162] Cox, *supra* note 157.

Playpen, was "so outrageous"[163] as to require dismissal.[164] The argument is based on the fact that in the thirteen days that the FBI hosted Playpen as a part of its investigation, "visitors to the site accessed, posted or traded at least 48,000 images, 200 videos and 13,000 links to child pornography."[165] It is maintained that the FBI went entirely against the Department of Justice's assertion that *each* time a pornographic image of a child is distributed or viewed, that child is re-victimized.[166] Ultimately, courts found the argument unpersuasive when weighed against the dire situation posed by the availability of exploitation material online.[167] To illustrate, Playpen had some 60,000 member accounts only a month after launching and 215,000 within a year of that time, with over 10,000 *new* visitors each week.[168] As important as it was to take Playpen down, one of the problems encountered by law enforcement is that taking down one site will not prevent more from popping up in its place.[169] Thus far, courts faced with these dismissal motions have recognized that the government was faced with a difficult choice and ultimately, its experts concluded that the best way to apprehend offenders and protect victims was to run the server for a limited amount of time.[170] As FBI Special Agent Dan Alfin said, "[i]t's a cat-and-mouse game, except it's not a game. Kids are being abused, and it's our job to stop that."[171] When requests for dismissals of charges are rejected, the next point of attack is the evidence behind those charges.

[163] Outrageous government conduct occurs where "the conduct of law enforcement agents is so outrageous that due process principles would absolutely bar the government from invoking judicial processes to obtain a conviction." United States v. Russell, 411 U.S. 423, 431–32 (1973).

[164] *See, e.g.*, Mot. & Memo ISO Mot. to Dismiss Indictment, U.S. v. Tippens, 2:15-cr-00274-RJB, at 6, 9 (Aug. 22, 2016), Dkt. No. 95 (arguing that "[i]t is no answer that the FBI did this as part of an effort to apprehend people. That end does not (and was never going to) justify the means.").

[165] 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/.

[166] *Id.*

[167] *See, e.g.*, United States v. Schreiber, No. 15-CR-377 (ENV), 2018 WL 276347, at *6 (E.D.N.Y. Jan. 3, 2018) ("[E]ven assuming there were alternative methods available, the government, in any event, is entitled to weigh the relative costs and benefits of the available array of investigatory approaches without being subject to judicial second guessing.").

[168] Joseph Cox, *The FBI's 'Unprecedented' Hacking Campaign Targeted over a Thousand Computers*, VICE: MOTHERBOARD (Jan. 5, 2016, 1:00 PM), https://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers.

[169] *See* discussion *supra* Part II.B.

[170] *See, e.g.*, United States v. Vortman, No. 16-cr-00210-teh-1, 2016 WL 7324987, at *5 (N.D. Cal. Dec. 16, 2016) (accepting the government's decision to run Playpen for a limited time in order to identify wrongdoers and help victims from further abuse).

[171] *Playpen Creator Sentenced to 30 Years*, *supra* note 143.

2. *Motions to Suppress Evidence from the NIT Warrant*

The two main arguments to suppress evidence obtained from the NIT Warrant center on challenges to the warrant's sufficiency under the Fourth Amendment and under Rule 41 of the Federal Rules of Criminal Procedure.[172] First, defendants argue that the NIT Warrant fails to meet the Fourth Amendment's requirements of probable cause and particularity.[173] Second, they reason that Magistrate Judge Buchanan did not have authority to authorize the NIT Warrant under Rule 41(b). Apart from four outliers,[174] courts across the country have denied the motions to suppress.[175] The various results of the suppression motions can be narrowed into four main categories. First, the NIT Warrant violated Rule 41(b), deployment of the NIT amounted to a warrantless search, and all evidence obtained from the NIT or subsequent warrants pursuant to the NIT must be suppressed.[176] Second, the NIT Warrant violated Rule 41(b), however, suppression of evidence was inappropriate based on: (1) technical violation; (2) good faith exception to the exclusionary rule; or (3) the exigent circumstances exception to a warrantless search.[177] Third, the NIT Warrant did not violate Rule 41(b) because it was authorized under either Rule 41(b)(1), Rule 41(b)(2), or Rule 41(b)(4).[178] Fourth, the NIT Warrant did not violate Rule 41(b), but even if it had, suppression of evidence would be unwarranted.[179]

The Fourth Amendment establishes that all warrants must be issued "upon *probable cause*, supported by Oath or affirmation, and

[172] *See, e.g.*, Unites States v. Tippens, No. 3:16-cr-05110-RJB, 2016 BL 446405, at *6 (W.D. Wash. Nov. 30, 2016) (addressing challenges based on probable cause and Rule 41).

[173] *See, e.g.*, *Vortman*, 2016 WL 7324987, at *6 (finding the NIT Warrant failed on both probable cause and particularity grounds).

[174] *See supra* note 158.

[175] *See, e.g.*, United States v. Taylor, 250 F. Supp. 3d 1215, 1222–23 (N.D. Ala. 2017):

> As of [April 24, 2017], at least 44 district courts have ruled on motions to suppress the information seized pursuant to the NIT warrant. Twelve of these courts have found that the warrant did not violate § 636(a) of the Federal Magistrates Act and/or Rule 41 . . . Twenty-two district courts have found that the warrant did violate § 636(a) and/or Rule 41(b), but that the violation did not warrant suppression. . . . [Six] have declined to decide whether the statute and/or the Rule authorized the warrant but found that exclusion was unwarranted regardless. . . . Four courts have suppressed the evidence.

[176] *See supra* note 158.

[177] *See, e.g.*, United States v. Perdue, 237 F. Supp. 3d 471, 478 (N.D. Tex. Feb. 17, 2017) (finding the Rule 41 violation in authorizing the NIT Warrant to be technical, rather than constitutional); United States v. Allen. No. 15-CR-620, 2017 WL 6397728, at *6 (E.D.N.Y. Dec. 14, 2017) (concluding the good faith exception to the exclusionary rule appropriate).

[178] *See, e.g.*, United States v. Jean, No. 5:15-cr-50087, 2016 WL 4771096, at *13 (W.D. Ark. Sept. 13, 2016) (holding the NIT to amount to a "tracking device" under Rule 41(b)(4)).

[179] *See, e.g.*, United States v. Epich, No. 15-CR-163-PP, 2016 WL 953269, at *2 (E.D. Wis. Mar. 14, 2016) ("Suppression of evidence is rarely, if ever, the remedy for a violation of Rule 41, even if such a violation has occurred.").

particularly describing the place to be searched and the persons or things to be seized.'"[180] Courts utilize a totality of the circumstances test[181] to determine whether there is probable cause by considering if there is a "fair probability" that evidence or contraband will be found in a *particular* place law enforcement seeks to search.[182] So far, defense attorneys[183] have failed in their efforts to convince courts that their clients logged onto Playpen without the intention to view child pornography (the triggering event of probable cause being logging onto Playpen which *clearly* hosts child pornography).[184] Courts have not accepted this argument, turning to the *extreme* unlikelihood of a user simply stumbling upon the page, much less, creating a username and logging on given the *multiple* affirmative steps required.[185] Defendants also argued the NIT Warrant did not meet the particularity requirement because it did not provide how Playpen "'unabashedly announce[d]' that it was an illegal child pornography site"[186] and because the logo on the first screen on Playpen described in the application was different from the one on the website when the NIT was deployed.[187] The view of most courts regarding these arguments can be summed up as: (1) the NIT Warrant was based on sufficient probable cause because the magistrate judge permissibly relied upon the FBI's conclusions that evidence of criminal activity was likely to be found; and (2) that the homepage image changed between when the FBI wrote its affidavit and when the NIT was deployed is immaterial to the underlying FBI conclusion because both images represented child pornography.[188]

Federal Rule of Criminal Procedure Rule 41(b), with limited exceptions, empowers federal magistrate judges with the authority to issue warrants within the judicial district the magistrate is in.[189] In the Playpen cases, the NIT Warrant authorized searches of computers

[180] U.S. CONST. amend. IV (emphasis added).

[181] *See* Illinois v. Gates, 462 U.S. 213, 214 (1983).

[182] United States v. Tippens, No. 3:16-cr-05110-RJB, 2016 BL 446405, at *6 (W.D. Wash. Nov. 30, 2016) (citing United States v. Gourde, 440 F.3d 1065, 1069 (9th Cir. 2006)).

[183] *See* Cox, *supra* note 157.

[184] *See* Transcript of Motions Hearing at 14, United States v. Michaud, No. 3:15-cr-05351-RJB (W.D. Wash. Jan. 22, 2016) (arguing that it is debatable whether the photo on the homepage of Playpen when the NIT was deployed was "lascivious" enough to indicate the content of the website as child pornography) [hereinafter Transcript of Motions Hearing].

[185] *See, e.g.*, United States v. Vortman, No. 16-cr-00210-TEH-1, 2016 WL 7324987, at *5 (N.D. Cal. Dec. 16, 2016) (describing the multiple affirmative steps that had to be taken to access Playpen).

[186] *Tippens*, 2016 BL 446405, at *6.

[187] Transcript of Motions Hearing, *supra* note 184, at 14 (arguing that the application for the NIT warrant described a different logo than that present when the NIT was deployed so the warrant failed for particularity).

[188] *See, e.g.*, *Tippens*, 2016 BL 446405, at *6–9 (addressing each point).

[189] *The Playpen Cases: Frequently Asked Questions*, *supra* note 65.

beyond the magistrate judge's own district, the Eastern District of Virginia.[190] The government has defended the NIT Warrant on the grounds that it was authorized under either Rule 41(b)(1), Rule 41(b)(2), or Rule 41(b)(4). Though nationwide prosecutions have produced differing opinions,[191] courts have generally come to one of three conclusions: (1) suppression is required because the NIT warrant was unlawfully issued;[192] (2) despite unlawful issuance of the NIT warrant, suppression is not the appropriate remedy;[193] or (3) suppression is not required because the NIT warrant was lawfully issued.[194] Each of the court orders granting suppression of evidence have been reversed on appeal so far.[195] Most courts have found the NIT Warrant violated Rule 41(b), but suppression of evidence would not be appropriate because: (1) the violation was technical; (2) the good faith exception applies; or (3) otherwise the exigency of harm caused by Playpen's operation.[196]

A Rule 41 violation can be substantive and constitutional or technical and procedural in nature.[197] If a court finds the NIT Warrant violates Rule 41, it has to consider whether that violation amounts to a fundamental error—as in a "clear constitutional [violation] warrant[ing] suppression"[198]—or a technical error "warrant[ing] suppression only if: (1) there is evidence of deliberate disregard of the rule, or (2) the defendants were prejudiced by the error."[199] The Playpen defendants argued the violation amounted to a constitutional level of "the cyber equivalent of the general warrants that were anathema to the Founders."[200] Specifically the argument is that the violation is constitutional in nature because the NIT enabled a warrantless search of their computers.[201] The government argues that even if the NIT Warrant

[190] *The Playpen Cases: Frequently Asked Questions*, *supra* note 65.

[191] United States v. Dzwonczyk, No. 4:15-cr-03134, 2016 WL 7428390, at *6 (D. Neb. Dec. 23, 2016).

[192] *See supra* note 158.

[193] *See supra* note 159.

[194] *See, e.g.*, United States v. Matish, 193 F. Supp. 3d 585, 593 (E.D. Va. Jun. 3, 2016) ("[A]ny potential defects in the issuance of the warrant or in the warrant itself could not result in constitutional violations, and even if there were a defect in the warrant or in its issuance, the good faith exception to suppression would apply.").

[195] *See supra* note 158.

[196] *See supra* note 177.

[197] *See* United States v. Rivera, No. 2:15-cr-00266, 2016 BL 442928, at *7–8 (E.D. La. Jul. 19, 2016) (explaining that suppression is warranted where Rule 41 is violated "only warranted if the defendant's constitutional rights were violated or the defendant experienced prejudice").

[198] United States v. Tippens, No. 3:16-cr-05110-RJB, 2016 BL 446405, at *8 (W.D. Wash. Nov. 30, 2016) (quoting United States v. Negrete-Gonzales, 966 F.2d 1277, 1283 (9th Cir. 1992)).

[199] *Id.*

[200] *Id.*

[201] *See, e.g.*, United States v. Werdene, 188 F. Supp. 3d 431, 443 (E.D. Pa. 2016) ("To demonstrate that the violation of Rule 41 was of constitutional magnitude, [defendant] must show a violation of his Fourth Amendment rights.").

is invalid, a warrant is not required to obtain an IP address, as one does not retain a reasonable expectation of privacy in information knowingly conveyed to third parties.[202] Defendants maintain the argument is inapposite in a situation where one actively masks this information by using Tor.[203] Some courts remain unpersuaded,[204] but others have found a meaningful distinction between one who knowingly exposes and purposefully takes steps to hide their IP address by using Tor.[205] Still, the difference between whether the Playpen defendants have a reasonable expectation of privacy in their masked IP addresses or not is inconsequential where courts determined that the NIT Warrant is valid, or suppression is inappropriate.[206]

Courts have ultimately decided that the reliance upon the NIT Warrant was objectively reasonable for multiple reasons. Specifically, the FBI affiant explained why the NIT was necessary, described the mechanics of deploying the NIT, described the nature of Playpen, and explained the particulars of what was to be searched by using the NIT.[207] Beyond the objective reasonableness, consideration was given to the ramifications of permitting culpable actors to circumvent responsibility weighed against "marginal deterrence, if any, that would result from suppression."[208] No court thus far has found that any potential deterrence to be gained from dismissal would outweigh the societal costs.[209]

[202] *See, e.g.*, United States v. Kahler, 236 F. Supp. 3d 1009, 1020 (E.D. Mich. 2017) (summarizing the government's argument "[relying] on the consensus among the Federal Courts of Appeal that there is no constitutionally recognizable privacy interest in an IP address."); *see also supra* note 17.

[203] *See, e.g.*, United States v. Jean, 207 F. Supp. 3d 920, 930–33 (W.D. Ark. 2016) (discussing the IP address issue at length).

[204] *See, e.g.*, United States v. Broy, 209 F. Supp. 3d 1045, 1053 (C.D. Ill. Sept. 21, 2016) (finding the defendant's sense of anonymity to "not negate the fact that, in order to gain that feeling of anonymity, he voluntarily disclosed his IP address to the operator of the first Tor node").

[205] *See, e.g.*, *Kahler*, 236 F. Supp. at 1021 ("Internet use pervades modern life. Law enforcement, acting alone, may not coerce the computers of internet users into revealing identifying information without a warrant, at least when the user has taken affirmative steps to ensure that third parties do not have that information.").

[206] *See, e.g.*, United States v. Johnson, 250 F. Supp. 3d 1215, 1236 (N.D. Ala. 2017) (even "[a]ssuming either a constitutional violation or prejudice under Rule 41(b) . . . the good faith exception to the exclusionary rule applies here").

[207] *See, e.g.*, United States v. Tippens, No. 3:16-cr-05110-RJB, 2016 BL 446405, at *9 (W.D. Wash. Nov. 30, 2016) ("relying on the [NIT] Warrant was objectively reasonable.").

[208] Order at 6, U.S. v. Kneitel, No. 8:16-cr-23-T-35JSS (M.D. Fla. Jan. 3, 2017), Dkt. No.158:

> [E]ven the cost of allowing this single defendant to go free—an individual who had been admittedly viewing and downloading child pornography for more than a decade . . . would far outweigh the benefit of preserving the precise adherence to a complicated and imprecise Rule application, especially where the Rule has now been modified.

[209] This assertion is based upon a thorough search of Westlaw and Bloomberg Law databases as of Feb. 1, 2018.

3. *Motions to Compel Source Code: "Disclosure is not currently an option."*[210]

After requests for dismissals proved unproductive, those fighting their indictments in the Playpen cases have sought to compel the government to provide the full NIT source code in discovery.[211] The government is required to produce certain "documents and objects" under Federal Rule of Criminal Procedure 16(a)(1)(E) provided that the information is "material to preparing the defense."[212] The discovery battles relating to the NIT source code, center on the amount of information the defense argues is "material" weighed against the government's efforts to protect the code as privileged for security reasons.[213] The government objected to supplying the full NIT source code but has provided parts of the code to experts,[214] maintaining that disclosure of the full source code is not necessary.[215] However, defendants have said that the information provided is not enough to ensure a fair trial.[216] A main reason for this argument, it appears, is a desire to have defense experts—fully equipped with appropriate security clearances—examine the code for potential defenses.[217] For example, the

[210] Gov't's Unopposed Motion to Dismiss Indictment Without Prejudice, at *2, United States v. Michaud, No. 3:15-cr-05351 (W.D. Wash. Mar. 3, 2017), Dkt. No. 227.

[211] *See* Joseph Cox, *The Other Reason the FBI Doesn't Want to Reveal Its Hackings Techniques*, VICE: MOTHERBOARD (Mar. 30, 2016, 5:00 AM), https://motherboard.vice.com/read/fbi-hacking-techniques.

[212] FED. R. CRIM. P. 16. *See, e.g.*, *Tippens*, 2016 BL 446405, at *12–13 ("The NIT code and other requested discovery is discoverable under Fed. R. Crim. P. 16 (a)(1)(E) because of its potential bearing on Defendants' motions, including the constitutional challenges to the NIT Warrant.").

[213] *See* Hennessey & Weaver, *supra* note 151.

[214] *See* Hennessey & Weaver, *supra* note 151 ("Knowledge of how the exploit works is the most sensitive part of an NIT-public disclosure not only risks losing the opportunity to use the technique against other offenders but would also permit criminals or authoritarian governments to use it for illicit purposes until a patch is developed and deployed."). Similarly to the case of *Scarfo*, *supra* Part III.B., the government has utilized § 4 of the Classified Information Procedures Act to keep a close grip over the code. *See, e.g.*, Tippens, 2016 BL 446405, at *13 ("[T]he Government made a sufficient showing to justify withholding the remaining portions of the NIT code and other discovery from Defendants."). For an explanation of the three-step framework utilized for evaluating CIPA § 4 motions, see United States v. Sedaghaty, 728 F.3d 885, 904 (9th Cir. 2013).

[215] *See, e.g.*, Decl. of FBI Special Agent Daniel Alfin in Support of Gov't's Motion For Reconsideration, ¶ 7, U.S. v. Michaud, No. 3L15 cr-05351-RJB (W.D. Wash. Mar. 28, 2016) Dkt. No. 166-2 (providing that "knowing how someone unlocked the front door provides no information about what that person did after entering the house. Determining whether the government exceeded the scope of the warrant thus requires an analysis of the NIT instructions delivered to Michaud's computer, not the method by which they were delivered.").

[216] *See* Joseph Cox, *Judge Rules FBI Must Reveal Malware It Used to Hack over 1,000 Computers*, VICE: MOTHERBOARD (Feb. 18, 2016, 2:02 PM), https://motherboard.vice.com/en_us/article/jpgmdd/judge-rules-fbi-must-reveal-malware-used-to-hack-over-1000-computers-playpen-jay-michaud ("[A]ccording to [defense expert, Vlad] Tsyrklevitch, the code was apparently missing several parts.").

[217] *See* Joseph Cox & Sarah Jeong, *FBI Is Pushing Back Against Judge's Order to Reveal Tor Browser Exploit*, VICE: MOTHERBOARD (Mar. 29, 2016, 7:10 AM),

NIT was not encrypted, opening up the possibility that the FBI's server was vulnerable to either third-party interception or tampering.[218] Experts, it is argued, need the full source code to determine areas of reasonable doubt for their clients, as well as to confirm the government only collected the information it professed to collect.[219]

Some motions to compel disclosure of the NIT code have resulted in dismissals. For example, the DOJ dropped its charges against Jay Michaud rather than reveal the full source code to an expert witness under narrow conditions.[220] The judge in Michaud's case said that although the technical details were "lost on [him]" he understood the underlying question of the motion: "[y]ou say you caught me by the use of computer hacking, so how do you do it? How do you do it? A fair question. And the government should respond under seal . . . and say here's how we did it."[221] However, a couple months later, after the government refused to comply with the order, the judge granted the government's motion to reconsider while simultaneously issuing sanctions against them.[222] Then, the court threw out all the evidence obtained from the NIT by granting a motion to suppress.[223] In response to the suppression order, the government first filed an interlocutory appeal, then withdrew its appeal and filed a motion to dismiss the indictment without prejudice.[224] In this motion, the government provided that it *had* to seek dismissal without prejudice because of its

https://motherboard.vice.com/en_us/article/gv5vy3/fbi-is-pushing-back-against-judges-order-to-reveal-tor-browser-exploit.

[218] *See* Decl. of Dr. Christopher Soghoian, ¶ 19, U.S. v. Matish, No. 4:16-cr-00016 (E.D. Va. Jun. 10, 2016), Dkt. No. 83-1. *But see* Hennessey & Weaver, *supra* note 151:

> The lack of encryption on the information transmitted . . . is a feature which enhances the chain of custody by providing visibility. For an unknown third party to tamper with this communication in a way which would have been prevented by encryption, that third party would need to have advance awareness of the FBI's activity, posses a valid login for the hidden site hosting the NIT . . . and simultaneously have a detailed profile of the target's computer.

[219] *See, e.g.*, Hennessey & Weaver, *supra* note 151 ("NITs offer the defense an opportunity to perform a detailed evaluation of the functionality, to determine what the NIT searched for, how it conducted the search, what data was seized, and the chain of custody.").

[220] *See* Gov't's Unopposed Motion to Dismiss Indictment Without Prejudice at 1, U.S. v. Michaud, No. 3:15-cr-05351, (W.D. Wash. Mar. 3, 2017); *see also* Transcript of Motions Hearing, *supra* note 184, at 18.

[221] Transcript of Motions Hearing, at 14, United States v. Michaud, No. 3:15-cr-05351-RJB (W.D. Wash. Feb. 17, 2016).

[222] Joseph Cox, *Judge Changes Mind, Says FBI Doesn't Have to Reveal Tor Browser Hack*, VICE: MOTHERBOARD (May 13, 2016, 7:50 AM), https://motherboard.vice.com/en_us/article/ezpp7e/judge-changes-mind-says-fbi-doesnt-have-to-reveal-tor-browser-hack.

[223] Order Denying Dismissal & Excluding Evidence, United States v. Michaud, No. 3:15-cr-05351 (W.D. Wash. May 25, 2016), Dkt. No. 212.

[224] *See* Gov't's Unopposed Mot. to Dismiss Indictment Without Prejudice, *supra* note 210, at 1–2.

unwillingness to disclose the NIT's full source code as "[d]isclosure [of the NIT's full source code] is not currently an option."[225]

If Michaud did commit the heinous acts he was accused of in his indictment then the fact that the government was unwilling to provide his expert access to the source code used to deploy malware is incredibly troubling. This move speaks to the value the FBI has attached to preserving the option to use the exploit in future investigations.[226] It undoubtedly was a difficult decision on the part of the government; one that is unable to be fully judged without all the facts surrounding it.[227] However, given the horrific nature of the crimes at issue, it is—from this vantage point—a maddening conclusion. The conflict between public transparency and the level of secrecy required to maintain effective investigation tactics is arguably at its most heated when the government is sooner willing to dismiss charges against an accused child abuser than to comply with a court order to produce information to ensure a fair trial.[228] Legislative response addressing and resolving these tensions is not only appropriate but desperately needed.

IV. TITLE III FOR GOVERNMENT HACKING

A. WARRANT AUTHORIZATION

The recent amendments to Rule 41(b) have prompted discussion of warrant authorization: namely, the authority of an un-elected body—the Advisory Rules Committee[229]—to authorize a new exception to warrant authorization without public consideration and the concern that some judges may not understand the technology that they are asked to approve

[225] *Id.*

[226] Michael Nunez, *FBI Drops All Charges in Child Porn Case to Keep Sketchy Spying Methods Secret*, GIZMODO (Mar. 6, 2017, 4:35 PM), https://gizmodo.com/fbi-drops-all-charges-in-child-porn-case-to-keep-sketch-1793009653 ("The FBI basically said they'd rather have [the defendant] go free than reveal the code, because if the code becomes publicly available, the ability to use this investigatory technique in the future is impaired.") (internal quotations omitted).

[227] *See, e.g.*, Hennessey & Weaver, *supra* note 151 (arguing "a compromise to one small part of an exploit could harm a vast array of incredibly important national interests. The question is one of balance and the ultimate determination is for a judge.").

[228] *See* Joseph Cox, *Lawyers: FBI Must Reveal Malware for Hacking Child Porn Users or Drop Its Case*, VICE: MOTHERBOARD (Apr. 25, 2016, 4:35 PM), https://motherboard.vice.com/en_us/article/ezpvp4/fbi-playpen-malware-NIT-jay-michaud.

[229] *See* Steven M. Bellovin et al., *Insecure Surveillance: Technical Issues with Remote Computer Searches*, COMMC'NS & PRIVACY UNDER SURVEILLANCE, Mar. 2016, at 14:

> In the US, the Judicial Conference—an administrative body of senior federal judges headed by the chief justice of the Supreme Court—frames policy guidelines for all federal courts. Proposed changes to federal rules are submitted, after public comment, by five advisory committees to the Judicial Conference's Standing Committee on Rules of Practice and Procedure, which upon its approval forwards them to the Supreme Court and Congress for final approval.

of in warrant applications. As discussed above, Rule 41 "governs the authorization of searches and seizures" in the United States.[230] As of December 31, 2016, Rule 41 now includes leave of a magistrate judge "to issue a warrant to *use remote access* to search electronic storage media and to seize or copy electronically stored information located within or outside that district if . . . the district where the media or information is located has been *concealed through technological means*."[231] This means that moving forward, a magistrate judge will have the authority to issue a warrant authorizing deployment of malware across the globe.[232] Beyond any foreign policy concerns of this authority,[233] there remains unease over the quick jurisdictional fix provided by a non-elected body.[234] A major criticism to these changes to Rule 41 is that the amendment assumes that hacking is a lawful activity when Congress has never actually authorized it.[235] Unlike wiretaps,[236] there is currently no legislative authority for government hacking of computers. This is not to say that the government's use of deploying malware in the course of their investigations is inherently unlawful. However, the level of secrecy is compounded by the lack of oversight and reliance upon judicial technological expertise in the absence of any guidance.

The Fourth Amendment itself does not address the powers of federal judges. However, case law illuminates the judiciary's importance as

[230] *Id.*

[231] FED. R. CRIM. P. 41(b)(6)(A) (emphasis added). For a background on the Rule change, see Appellee's Opening Brief, United v. Levin, No. 16-1567 (1st Cir. Feb. 2017), 2017 WL 512509, at *2:

> In April 2013, a decision was issued from the Southern District of Texas that denied a warrant request to conduct a remote access search of a computer in an unknown location. *In re Warrant to Search a Target Computer at Premises Unknown*, 758 F. Supp. 2d 753 (S.D. Tex. 2013) . . . That decision prompted the Department of Justice to formally request an amendment to the Federal Rules of Criminal Procedure.

[232] For a criticism of this authority, see Brief of Amici Curiae Electronic Frontier Found. & Am. Civ. Liberties Union of Mass. In Support of Defendant-Appellee & Affirmance, United States v. Levin, No. 16-1567, at 3 (1st Cir. Feb. 10, 2017) ("A warrant that authorized the search of hundreds or thousands of homes, without identifying specific buildings or specifying where those buildings were located, would be rejected out of hand even if those searches were limited to identifying the person residing there."); Robyn Greene, *Congress Must Pass the Stopping Mass Hacking Act*, NEW AM. (June 1, 2016), https://www.newamerica.org/oti/blog/congress-must-pass-stopping-mass-hacking-act/.

[233] For a discussion on the implications of this, see Ghappour, *supra* note 57.

[234] For criticisms of the Rule 41 changes, see, for example, Bellovin et al., *supra* note 229, at 14 (finding the changes to Rule 41 to "confuse legitimate uses of location-anonymizing software with nefarious activity, and . . . likely . . . be both intrusive and damaging"); Press Release, Ron Wyden, United States Senator, Wyden: Untested Government Mass Hacking Techniques Threaten Digital Security, Critical Infrastructure (June 30, 2016), https://www.wyden.senate.gov/news/press-releases/wyden-untested-government-mass-hacking-techniques-threaten-digital-security-critical-infrastructure ("Nobody can see years into the future to tell us what mass hacking by criminals or by law enforcement will be capable of doing. And if these changes go into effect, there will be no guidelines in place to ensure that the privacy and security of Americans are being protected.").

[235] *See* Greene, *supra* note 232.

[236] 18 U.S.C. §§ 2510–2022 (2016).

gatekeepers between law enforcement and individual civil liberties. Below is an excerpt from an evidentiary hearing in one of the Playpen cases (since dismissed by motion of the government to avoid disclosure of the source code) where a U.S. District Court Judge seeks clarity regarding what the NIT did:

> THE COURT: Do the FBI experts have any way to look at the NIT information other than going to the server?
>
> MR. FIEMAN: Your Honor, they don't go to the server.
>
> THE COURT: Where do they go? How do they get the information?
>
> MR. FIEMAN: They get it from Mr. Michaud's computer.
>
> THE COURT: They don't have his computer.
>
> MR. FIEMAN: That's what the NIT is for.
>
> THE COURT: You see, this is what is confusing to me. It has a lot to do with where the search occurred. How do they find information? Maybe you need to call a witness on these things. . . I want to know what the user has to do to trigger this NIT, if anything. Then I want to know what does the FBI guy do to find out where—the information that the NIT provides, how does he get that? I suppose there is somebody sitting in a cubicle somewhere with a keyboard doing this stuff. I don't know that. It may be they seed the clouds, and the clouds rain information. I don't know. . . I don't want the detail. It wouldn't mean anything to me anyway. But I understand enough to know that if you want to see something on your computer, you have to turn it on and hit the right strokes, or else you are just in there playing solitaire or something. I don't care what the strokes are. I don't care about that. I just want to know what's available and how they would do it.[237]

The above exchange would never occur in the context of a warrant to search a house, a car, or a store because the authority responsible for evaluating the legal elements of a valid warrant understand how police officers search physical spaces. Without that understanding, can a judge make a meaningful decision? While the dialogue above was taken from a hearing of a district court judge and does not involve consideration of a warrant application, it serves as a perfect example of why the amendments to Rule 41 warrant pause. A potential issue here is that those authorized to issue searches like those under the NIT Warrant do not necessarily understand the technology that they are authorizing.[238] The technology involved here is complex and the government utilizes sophisticated investigative tactics. Technology grows at a faster rate than the law can handle and it is not a slight to the intelligence of judges to call their technological expertise into question.

[237] Transcript of Motions Hearing, *supra* note 184, at 50.

[238] Joseph Cox, *Judge in FBI Hacking Case Is Unclear on How FBI Hacking Works*, VICE: MOTHERBOARD (Jan. 27, 2016, 9:50 AM), https://motherboard.vice.com/read/judge-in-fbi-hacking-case-is-unclear-on-how-fbi-hacking-works.

If judges do not understand the technology then they cannot understand the government action that they authorize. This is not to suggest that judges are unable to learn what they need to know to make competent decisions in authorizing warrants. Judges are tasked with learning convoluted and complicated matters in the course of their careers. However, in many settings, judges benefit from the adversarial nature of the legal system by hearing from opposing sides. When a warrant is requested from a judge, there only is the government before the court. Joseph Cox, a journalist for *Vice Motherboard*, who has written extensively on government hacking concluded that although some judges in cases involving NITs do not understand how hacking works, the fault is not placed squarely on the courts as "it's arguably a problem stemming from how the [government] ha[s] framed and referred to NITs in legal documents."[239] Either way, instead of critically evaluating the operation that they are being asked to authorize, judges, as finders of fact, may have to defer to the experts, in this instance the FBI, on issues of technological fact.[240]

To address concerns of technological competence, stringent requirements for Continuing Judicial Education should be mandated for all federal judges at the magistrate and district level.[241] Above all, these requirements should focus on ensuring competency on government hacking and surveillance technology as it pertains to the authorization of warrants. An alternative option is that judges who complete a set amount of hours or specific courses could be certified to handle warrants requiring a specialized understanding of investigative tools that go beyond physical spaces. This standard ensures that those tasked with the authority are well equipped with the necessary foundation to evaluate applications before their courts. Regardless of the solution, it is paramount that those vested with the authority to authorize warrants which lead to deployment of malware are in a position to consider the request on all its levels. While venue issues are resolved with the updated Rule 41,[242] across the board judicial understanding of the technology they are tasked to authorize will not be without further discussion.

[239] *Id.*; *see also* MACKEY ET AL., *supra* note 27, at 7 (describing the shortcomings of metaphors used to compare IP addresses to physical street addresses or license plates in warrant applications).

[240] *See* Robert M. Chesney, *National Security Deference*, 95 VA. L. REV. 1361, 1367 (2009).

[241] Currently, "[t]here are no mandatory educational requirements or standards for federal judges, but the majority take advantage of Center offerings." INT'L JUDICIAL RELATIONS OFFICE, FED. JUDICIAL CTR., EDUC. AND RESEARCH FOR THE U.S. FED. COURTS (2014), https://www.fjc.gov/sites/default/files/2015/About-FJC-English-2014-10-07.pdf.

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

B. WHO WILL WATCH THE WATCHMEN?

Despite that the FBI has used malware for almost two decades, law enforcement has yet to seek clear authority from Congress to use this technology.[243] Law enforcement instead seeks judicial sanction to utilize its malware "on an ad hoc basis" by applying, vaguely, for search warrants under Rule 41.[244] Executive restraint, while a good thing, is not enough on its own. One of the Playpen courts found the NIT Warrant to be proper, in part, because the warrant authorized the FBI to do more than the FBI did: namely, the FBI chose not to deploy the NIT on a target until that target logged onto Playpen, however, the warrant authorized deployment upon arrival to the hidden service.[245] The fact that the warrant authorized more than what the agents did should not make people feel better because a court of law did not impose that restraint.[246] But, even more so than the capriciousness of relying upon executive restraint, "[g]overnment action that actively sabotages or even collaterally undermines digital security is too important to be left open to executive whim."[247] After all, a fundamental aspect of American government is the checks and balances of government powers.

Unlike other mediums of communications, the dark web is no man's land. The level of secrecy in government hacking, while necessary to a degree, is complicated by the lack of oversight. Government hacking as an investigatory tool implicates apprehensions which cannot be resolved without public awareness and legislative discussion regarding the means of use and extent of judicial oversight. There must be a discussion of our lawmakers in order for the liberties of all people to be safeguarded. Congress has all the tools it needs to do so. Chris Soghoian, provides, "[i]f

[243] *See* Motion to Unseal Court Docket Sheet at 2, *In re* Sealed Docket Sheet Associated With Malware Warrant Issued on July 22, 2013, No. 1:16-cv-03029-JKB (D. Md. Aug. 29, 2016) (pertaining to the Freedom Hosting investigation).

[244] *Id.*

[245] *See* Opinion & Order at 8, United States v. Matish, No. 4:16-cr-00016-HCM-RJK (E.D. Va. Jun. 23, 2016) (explaining that "the FBI deployed the NIT in a much narrower fashion than what the warrant authorized").

[246] *See, e.g.*, Katz v. United States, 389 U.S. 347, 356–57 (1967):

> It is apparent that the agents in this case acted with restraint. Yet the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer. . . . In the absence of such safeguards, this Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end.

[247] Andrew Crocker, *What to Do About Lawless Government Hacking and the Weakening of Digital Security*, ELEC. FRONTIER FOUND. (Aug. 1, 2016), https://www.eff.org/deeplinks/2016/08/what-do-about-lawless-government-hacking-and-weakening-digital-security.

Congress decides this is a technique that's perfectly appropriate, maybe that's OK. But let's have an informed debate about it."[248]

The FBI is believed to have deployed the NIT in the Playpen cases upon the thousands by exploiting a Tor browser vulnerability.[249] As discussed above, the full source code of the NIT and the exploit used to deploy it, is unknown to the public as well as defendants because the government has refused to release the full code.[250] The government maintains that it is unwilling to do so at this time because of the importance of the code remaining secret. This is even after at least one of the Playpen defendants secured a defense expert with top level security clearance specifically to accommodate the sensitive nature of the discovery requested.[251]

Governments, the United States included, search for vulnerabilities like the one used in the Playpen investigation to exploit them to collect intelligence or for purposes of surveillance.[252] These vulnerabilities are stored by governments, again, the United States included, for future use.[253] This is problematic because once a vulnerability is found there is a risk that it may be discovered by others who may use the vulnerability for malicious purposes.[254] While the government openly recognizes the dire threats of cybercrime,[255] it continues to engage in activities which, without oversight, may put citizens at further risk because by taking "step[s] to create, acquire, stockpile or exploit weaknesses in digital security, it risks making us all less safe by failing to bolster that security."[256] Perhaps the saying that "guns don't kill people, people do" would be appropriate here, however, it would miss the point entirely in terms of exploits. The analogy would possibly work in a situation where a police officer finds a gun on the sidewalk, leaves it there in case she may need it in the future, all the while leaving open the possibility of discovery

[248] Poulsen, *supra* note 48.

[249] *The Playpen Cases: Frequently Asked Questions*, *supra* note 65.

[250] *See* Lily Hay Newman, *The Feds Would Rather Drop a Child Porn Case than Give Up a Tor Exploit*, WIRED (Mar. 7, 2017, 9:00 AM), https://www.wired.com/2017/03/feds-rather-drop-child-porn-case-give-exploit; Government's Unopposed Motion to Dismiss Indictment Without Prejudice, United States v. Michaud, No. 3:15-cr-05351-RJB (W.D. Wash. Mar. 3, 2017) ("Because the government remains unwilling to disclose certain discovery related to the FBI's deployment of a [NIT] as part of its investigation into the Playpen child pornography site, the government has no choice but to seek dismissal of the indictment.").

[251] Third Motion and Memorandum of Law in Support of Motion to Compel Discovery at 1 n.3, United States v. Michaud, No. 3:15-cr-05351 (W.D. Wash. Jan 14, 2016).

[252] *See* Crocker, *supra* note 247.

[253] Crocker, *supra* note 247.

[254] Crocker, *supra* note 247.

[255] Leslie R. Caldwell, *Legislative Proposals to Protect Online Privacy and Security* (Mar. 9, 2015), https://www.justice.gov/archives/opa/blog/legislative-proposals-protect-online-privacy-and-security.

[256] Crocker, *supra* note 247.

by nefarious figures. This absurd hypothetical is neither believable nor an entirely accurate analogy. But its absurdity perhaps drives the point across. By exploiting security flaws, the government is not leaving weapons on the street, rather, they are discovering things that could be used as weapons, exploiting them in their own investigations, and leaving that possibility open for others to do the same. Here, there is more at stake than the invasion of privacy of the "bad guys." There are undeniable benefits to the use of government malware, in fact, the use may be entirely necessary in today's world. However, there are also costs, and those costs grow exponentially when there is no oversight. Without rules and oversight, the question becomes: who will watch the watchmen?

C. UNCHARTED STATUTORY TERRITORY

"Electronic surveillance succeeds because it is secret."[257] The element of secrecy surrounding a particular application of surveillance thus takes priority over the law's purpose to limit executive discretion.[258] In addition to the Fourth Amendment, three statutes collected under the Electronic Communications Privacy Act of 1986 ("ECPA") are crucial to that end.[259] Title I of the ECPA, also known as the Wiretap Act, or Title III,[260] regulates the interception of transmitted communications.[261] Title II of the ECPA, also known as the Stored Communications Act governs how communication service providers may disclose the metadata and contents of customers' stored information.[262] Title III pertains to pen registers and trap trace devices.[263]

While some critics take issue with the fact that the government engages in hacking at all, it is undeniable that this form of surveillance has a place in investigation of crimes as well as protection of national security.[264] Furthermore, as freedom is not limitless, "it seems only proper that the vast freedoms of the Internet be subject to the same rule of law and protections that we accept for the rest of society."[265] That said, the use of hacking as an investigative tool on behalf of the government is

[257] Crocker, *supra* note 76.

[258] Crocker, *supra* note 76.

[259] U.S. DEP'T OF JUSTICE, COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS ix (2009).

[260] *See* U.S. DEP'T OF JUSTICE, *Title III of The Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act)*, BUREAU OF JUSTICE ASSISTANCE, https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1284 (last updated Sept. 19, 2013).

[261] Title I of the ECPA is codified at 18 U.S.C. §§ 2510–2522 (2012).

[262] Title II of the ECPA is codified at 18 U.S.C. §§ 2701–2712 (2012).

[263] Title III of the ECPA is codified at 18 U.S.C. §§ 3121–3127 (2012).

[264] *See* Jonathan Mayer, *You Can't Backdoor a Platform*, WEB POL'Y (Apr. 28, 2015), http://webpolicy.org/2015/04/28/you-cant-backdoor-a-platform.

[265] Editorial Board, *supra* note 41.

not *per se* unconstitutional,[266] as "[h]acking—just like kicking down a door and looking through someone's stuff—is a perfectly legal tactic for law enforcement officers, provided they have a warrant."[267] However, unlike kicking down a door, a problematic aspect of warrants in the context of hacking is that issues arise when the places to be searched are less clear cut than, say, a public phone booth.[268] Furthermore, the act deals with uncharted statutory territory.

Congress should enact a comprehensive statute like Title III for government hacking to set clear standards and guidance for law enforcement, thereby legitimatizing its hacking operations and safeguarding individual liberties through oversight.[269] Andrew Crocker, a Staff Attorney with the Electronic Frontier Foundation, has advocated for such a move, providing "[j]ust as with wiretapping, we should be mindful of the need for both constitutional and statutory law to keep up with the use of hacking for surveillance."[270] Unlike traditional warrants, wiretap orders, authorized by Title III warrants, are far more stringent.[271] In addition to the high bar law enforcement needs to meet to obtain a Title III warrant,[272] once obtained, Title III warrants require minimization procedures to be put in place to ensure the least amount of intrusion possible.[273] Furthermore, the public receives annual updates on the number and type of wiretaps utilized by the government as a mandate of the statute.[274] A Title III for government hacking could mandate similar protections by: setting a high bar for issuance of hacking orders, ensuring utilization of malware as a last resort when other, less intrusive means, are insufficient, compelling minimization requirements to curtail

[266] *See, e.g.*, *Government Hacking and Subversion of Digital Security*, *supra* note 75, at 575 n.16 ("[M]y view is that hacking can be a legitimate and effective law enforcement technique. I also use the term to promote consistency and avoid ambiguity.").

[267] McLaughlin, *supra* note 111.

[268] Katz v. United States, 389 U.S. 347, 353–54 (1967).

[269] *See, e.g.*, Crocker, *supra* note 247 ("Given the dangers posed by government malware, the public would likely be better served by the enactment of affirmative rules, something like a 'Title III for Hacking.'").

[270] Crocker, *supra* note 76.

[271] *See* Carrell, *supra* note 81, at 208; U.S. DEP'T OF JUSTICE, *supra* note 260 (providing that the Wiretap Act "prohibits the unauthorized, nonconsensual interception of 'wire, oral, or electronic communications' by government agencies as well as private parties[;] establishes procedures for obtaining warrants to authorize wiretapping by government officials, and[;] regulates the disclosure and use of authorized intercepted communications by investigative and law enforcement officers").

[272] *See* 18 U.S.C. § 2518 (2012) (detailing the processes and procedures for applying and issuing wiretap orders); *29. Electronic Surveillance—Title III Affidavits*, U.S. DEP'T OF JUSTICE, https://www.justice.gov/usam/criminal-resource-manual-29-electronic-surveillance-title-iii-affidavits (last updated Jan. 2018).

[273] *See* 18 U.S.C. § 2515 (2012) (explaining minimization of interference).

[274] *See* 18 U.S.C. § 2519 (2012) (providing public reporting requirements).

information obtained and risk posed, requiring public reporting on an annual basis, and other specifications as Congress deems appropriate.[275]

The real concern is regarding *how* online surveillance is conducted, rather than *that* it is conducted at all.[276] The problem is that unlike other forms of technology (for example, phones), there is currently no statutory framework in place to guide law enforcement or the public. It is beyond question that law enforcement needs to apprehend individuals who use Tor and Virtual Private Networks known as "VPNs"[277] to access the illicit sites at issue in Operation Torpedo, and Operation Pacifier. Wrongdoers cannot be permitted to evade justice through technological advances, so law enforcement must be empowered to prevent such evasion.[278] However, it is the *means* of apprehension, not the ends, which give pause. It is especially difficult to focus upon this concern in the context of investigations tackling child pornography, given the unforgiveable nature of crimes against children. Legislative intervention is increasingly more necessary as technology grows and it becomes clear that the constitutional protections in place are not enough alone to ensure that privacy and security considerations are not swept to the side.

CONCLUSION

It is problematic that the government uses its authority to invade personal spaces within the home without oversight. This is not to suggest that the aims of law enforcement in using NITs are unimportant, nor is it an assertion that law enforcement should be prevented from apprehending offenders. No one should be empowered to break the law just because they may be technologically savvy enough to avoid detection, especially when committing arguably the most heinous crime one can

[275] Crocker, *supra* note 76. *See* Freiwald, *supra* note 4:

> In the wake of decades of hearings, numerous rejected bills, and intense public debate, the Wiretap Act achieved a workable compromise that has largely stood the test of time. All branches of government and countless experts had input into the design of the Wiretap Act. It provides a comprehensive scheme that strictly limits law enforcement's use of electronic surveillance and provides several mechanisms to ensure that.

[276] *See* Kate Knibbs, *The FBI Has Its Own Secret Brand of Malware*, GIZMODO (Apr. 2, 2015, 11:45 AM), https://gizmodo.com/the-fbi-has-its-own-secret-brand-of-malware-1694821520 ("The extent to which we're being kept in the dark about government spyware is not necessary.").

[277] *What Is a VPN? And Why You Should Use a VPN on Public Wi-Fi*, NORTON BY SYMANTEC, https://us.norton.com/internetsecurity-privacy-what-is-a-vpn.html (last visited May 7, 2018):

> A virtual private network (VPN) gives you online privacy and anonymity by creating a private network from a public Internet connection. VPNs mask your [IP] address so your online actions are virtually untraceable. Most important, VPN services establish secure and encrypted connections, guaranteed to provide greater privacy than even a secured Wi-Fi hotspot.

Id.

[278] *See* United States v. Skinner, 690 F.3d 772, 778 (6th Cir. 2012).

commit (crimes against children). However, "[i]n our society, the rule of law sets limits on what government can and cannot do, no matter how important its goals."[279] As Justice Brandeis warned in his *Olmstead* dissent, "[i]f the government becomes a lawbreaker, it breeds contempt for law; it invites every man to become a law unto himself; it invites anarchy."[280] For laws to work, people must respect the law. If law enforcement is seen as bending the rules to do its job, regardless of how significant that job is, this will breed a view of their operations as illegitimate and, by extension, will give the entire government the shadow of illegitimacy.

Right now, it is easy not to care about the lack of legislative oversight over government hacking, because the only people implicated (as far as the public knows) are those exploiting children. However, that does not mean we should ignore the implications of establishing far reaching precedents, nor ignore suggestions of overstep even in the pursuit of those viewing pure contraband. The descriptions of the content available on these despicable websites makes it very easy to forget the potential repercussions of allowing law enforcement unlimited power to apprehend people behind their computer screens without oversight. Even a cursory reading of the unsealed applications and affidavits in the Playpen cases is enough to illustrate the importance of apprehension.[281] The technology requested by law enforcement is left arguably vague but the enemy illustrated by the applications is anything but.

Online browsing activity weaves an intricate web stringing together all the virtual places visited from the comfort of our physical and private locations. This web paints its own kind of picture: it identifies traits and stockpiles information; it tracks activities, purchases, and real world locations; and it provides a way to pinpoint a source to criminal behavior. Many people do not think about the trail left behind with each click of a link, or search in an engine. But some take elaborate measures to circumvent tracking to visit online spaces in the dark. This circumvention is in many ways a legitimate reaction to the magnitude of privacy concerns posed by the digital revolution and an important tool in combatting those concerns. However, it is also a tool which empowers predators like those in the Playpen cases to abuse anonymity and elude capture. In turn, it has caused the government to take steps that should give one pause when confronting the repercussions of due process.

[279] Crocker, *supra* note 247.

[280] Olmstead v. United States, 277 U.S. 438, 485 (1928) (Brandeis, J., dissenting).

[281] *See, e.g.*, Application & Affidavit of FBI Special Agent Douglas Macfarlane, *In re* Search of Computers that Access upf45jv3bziuctml.onion, No. 1:15-SW-89 (E.D. Va. Feb. 20, 2015) (the application which led to the authorization of the NIT Warrant).

Unlike the characters in Mary Howitt's poem, *The Spider and the Fly*, the prey and the predator are muddled by situations like the one in the Playpen cases. There may be something to be said for the poetic justice in the progression of the predator becoming the prey, however, we do not live in a lawless society where the ends can always justify the means. Just as it is easy to be caught up in the dragnet, it is not difficult to find ways in which to excuse the government's behavior in order to reconcile their ensnaring the "bad guys." This is dangerous thinking. Without Congressional intervention to outline the boundaries of the use of the grey in these criminal investigations, the government risks losing much more than a trial, it risks the loss of legitimacy.

While the premise of prioritizing the protection of children over all else—including over the due process rights of predators—has moral merit, it does not fit into the legal fabric of the United States. There is much more at stake than invasions on those committing the "Crime Everyone Hates."[282] The U.S. criminal justice system is based upon a presumption of innocence; the law protects everyone, from the most loathsome offender to the purest innocent. The Constitution does not pick and choose who is worthy beyond that of citizenry and requisite contacts.[283] Even if that were not so, and one were to draw the line of due process at child pornography, what is to prevent that line from moving further and further until we live in a society where the mere accusation of any crime is enough to strip one of their entitlement to due process? One person may easily draw a line for sex offenders, specifically child predators, while the next person may easily do the same for non-violent drug offenders. Whose line prevails here? Unfortunately, drawing lines in the sand is not a viable solution. In the interim, while distracted by the waves, we risk erosion of civil liberties.

[282] In his blog, Scott Greenfield refers to Michaud's charges as the "Crime Everyone Hates" in discussing the implications of the possibility that the Government would rather dismiss charges against him than disclose the Tor Browser exploit. Scott Greenfield, *Is "Under No Circumstances" Acceptable, Judge?*, SIMPLE JUSTICE BLOG (Apr. 26, 2016), https://blog.simplejustice.us/2016/04/26/is-under-no-circumstances-acceptable-judge.

[283] *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 269–74 (1990) (discussing who "the people" are under the Fourth Amendment).