NITS A NO-GO: DISCLOSING EXPLOITS AND TECHNOLOGICAL VULNERABILITIES IN CRIMINAL CASES

RUPINDER K. GARCHA*

Network investigative techniques (NITs) are law enforcement tools that allow the government to hack into targeted computers by exploiting technological vulnerabilities. NITs have succeeded in identifying and locating criminal actors operating on the Dark Web where traditional investigative techniques have failed. They play a critical role in the investigation of cybercrime and in the national security sphere. But disclosure of a NIT's code can render it useless and jeopardize government operations that rely on that code. In numerous federal cases, criminal defendants have sought access to NIT code, and courts have had to decide whether the government must disclose the code. The government's interest in confidentiality is inherently at tension with criminal defendants' right to discovery and information material to their defense.

In order to make informed decisions about disclosure, courts must be cognizant of the equities at stake and understand technical details about NITs. Courts can better equip themselves by holding ex parte and in camera proceedings, and appointing experts to augment their understanding of technical issues. These procedures can ensure that the government is held accountable, defendants' rights are protected, and NIT code is preserved. As the Dark Web expands, cybercrime is likely to become more pervasive, and criminal actors will devise more sophisticated means of anonymizing their presence online. Law enforcement will have to respond creatively and courts must be prepared to tackle novel issues that straddle technology and law.

 J.D., 2018, New York University School of Law; B.A., 2013, Haverford College. Thank you to Professor Lisa O. Monaco for invaluable input and guidance from day one. Many thanks to Professor Harry First, Professor Randy Milch, and Zachary Goldman for helpful comments, suggestions, and criticism. I would also like to thank the Garcha family for their endless support, particularly Jasminder Garcha. And special thanks to the editors of the *New York University Law Review*, especially Alexandra Ferrara, Julian Clark, Ryan Hanley, and Hillel Buechler.

Introduction

In today's ever-connected world, the Internet and technology are integral to almost every aspect of our lives. While this interconnectedness and fast-paced technological innovation have accelerated globalization and improved the quality of life, they have also contributed to the growth of the Internet underworld—the Dark Web[1]—where traditional crimes have taken on a cyber dimension and flourish undetected.[2] Criminals in cyberspace evade "law enforcement's most advanced electronic surveillance tools" by using anonymizing software.[3] Not surprisingly, U.S. law enforcement often lacks the technical ability to investigate cybercrime.[4]

---

[1] *See* Daniel Sui et al., Wilson Center, The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box 7 (2015) (noting that "[a]dvances in secure/anonymous web hosting services, cryptocurrency/Dark Wallet, and development of crimeware" have contributed to the growth of the Dark Web). The Dark Web refers to a "network supporting cryptographically hidden sites," Daniel Moore & Thomas Rid, *Cryptopolitik and the Darknet*, 58 Survival 7, 15 (2016), which may be accessed anonymously. *Id.* at 16.

[2] *See* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 Stan. L. Rev. 1075, 1077–78 (2017) (discussing the upward of a million drug deals that took place on the Silk Road, an online black marketplace that guaranteed the anonymity of transactions for illicit goods and services beyond the reach of law enforcement); Cara McGoogan, *Dark Web Browser Tor Is Overwhelmingly Used for Crimes, Says Study*, Telegraph (Feb. 2, 2016, 2:35 PM), http://www.telegraph.co.uk/technology/2016/02/02/dark-web-browser-tor-is-overwhelmingly-used-for-crime-says-study/ (stating that "[t]here is an 'overwhelming' amount of illicit and illegal content on the dark web").

[3] Ghappour, *supra* note 2, at 1078; *see also id.* at 1079 ("The use of the dark web by criminal actors . . . enables secret, untraceable criminal activity to take place at scale.").

[4] *See* James B. Comey, Dir., Fed. Bureau of Investigation, Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course? (Oct. 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course ("[T]he law hasn't kept pace with technology, and this disconnect has created a significant public safety problem. . . . Those charged with protecting our people aren't always able to access the evidence we need to prosecute crime . . . . [W]e often lack the technical ability to do so.").

However, in December 2014, federal investigators got lucky.[5] A foreign law enforcement agency notified investigators that it had located the server[6] hosting the Dark Web child pornography website, Playpen, in the U.S.[7] The FBI seized the server and the website, but could not identify individuals accessing Playpen and posting illicit content.[8] In a controversial move, the FBI resolved to continue running the website,[9] and obtained a court-authorized warrant to employ a "network investigative technique" (NIT) to identify Playpen visitors.[10] A NIT is a surveillance tool that circumvents Dark Web users' anonymizing software and allows the government to "remotely access[ ] and install[ ] malware on a computer without the permission of its owner or operator."[11] Once in control of a computer, the NIT retrieves identifying information, including an IP address, which allows the FBI to pinpoint the computer's location. The Playpen NIT warrant essentially sanctioned *government hacking*.[12]

---

[5] *See 'Playpen' Creator Sentenced to 30 Years*, FBI (May 5, 2017), https://www.fbi.gov/news/stories/playpen-creator-sentenced-to-30-years (noting that an FBI investigator noticed Playpen's IP address in December 2014).

[6] Websites are hosted—or stored—on web servers. Servers are computers "designed to process requests and deliver data to another computer over the internet or a local network." Bradley Mitchell, *Servers Are the Heart and Lungs of the Internet: The Internet Wouldn't Exist Without Servers*, LIFEWIRE, https://www.lifewire.com/servers-in-computer-networking-817380 (last updated Feb. 6, 2018). Specifically, Internet browsers connect to web servers to deliver users the web pages they see. *Id.*

[7] Joseph Cox, *An Admin's Foolish Errors Helped the FBI Unmask Child Porn Site 'Playpen'*, VICE: MOTHERBOARD (May 16, 2016, 11:00 AM), https://motherboard.vice.com/en_us/article/nz7e8x/an-admins-foolish-errors-helped-the-fbi-unmask-child-porn-site-playpen.

[8] *See* Susan Hennessey & Nicholas Weaver, *A Judicial Framework for Evaluating Network Investigative Techniques*, LAWFARE (July 28, 2016, 10:17 AM), https://www.lawfareblog.com/judicial-framework-evaluating-network-investigative-techniques (explaining that the FBI could not "determine the physical location of individuals who were accessing and posting child pornography").

[9] *See* Joseph Cox, *Here Is the Warrant the FBI Used to Hack over a Thousand Computers*, VICE: MOTHERBOARD (Mar. 8, 2016, 10:50 AM), https://motherboard.vice.com/en_us/article/aekkwk/here-is-the-warrant-the-fbi-used-to-hack-over-a-thousand-computers (noting that the FBI continued to run the site "from its own servers for 13 days, and hacked over a thousand computers that visited it").

[10] *See id.* (describing how the warrant for the NIT allowed the FBI to collect individuals' real IP addresses, computer operating system information, and other identifying information).

[11] Ghappour, *supra* note 2, at 1079.

[12] *See id.* ("The term 'network investigative technique' is a euphemism for law enforcement hacking."); Orin S. Kerr & Sean D. Murphy, Essay, *Government Hacking to Light the Dark Web: What Risks to International Relations and International Law?*, 70 STAN. L. REV. ONLINE 58, 58 (2017), https://www.stanfordlawreview.org/online/government-hacking-to-light-the-dark-web/ (noting that government hacking can occur "as part of legitimate criminal investigations"); Orin Kerr, *Government 'Hacking' and the Playpen Search Warrant*, WASH. POST: VOLOKH CONSPIRACY (Sept. 27, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/09/27/government-hacking-and-the-

Since shutting down the notorious website, the government has pursued charges against at least 137 individuals around the country (the "Playpen cases"),[13] including Jay Michaud. Michaud, a school administrator from Washington, was arrested in 2015 for viewing child pornography on Playpen,[14] but in 2017, federal prosecutors dismissed the case.[15] They had the evidence to secure a conviction, but were "graymailed."[16] Graymail is a tactic where the defense threatens to reveal classified or highly sensitive government information if prosecuted, in an effort to force the government to dismiss the case.[17] In numerous Playpen cases, defendants have sought access to the complete NIT code in the hopes that courts will compel the government to disclose the code, and that the government will then dismiss the case because it prefers to maintain the confidentiality of the NIT code.[18]

What is at stake? NITs are invaluable in investigating cybercrime and identifying "criminal suspects who use anonymizing software to obscure their [physical] location."[19] The confidentiality of NIT code, or at least parts of NIT code, is important because the code reveals

---

playpen-search-warrant/?utm_term=.40b3fb7da3ff (analyzing the "legality of a single search warrant that was used to search the computers of many visitors to a child pornography website").

13 Hennessey & Weaver, *supra* note 8.

14 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/.

15 *Id.*

16 Hennessey & Weaver, *supra* note 8.

17 *See* EDWARD C. LIU & TODD GARVEY, CONG. RESEARCH SERV., R41742, PROTECTING CLASSIFIED INFORMATION AND THE RIGHTS OF CRIMINAL DEFENDANTS: THE CLASSIFIED INFORMATION PROCEDURES ACT 1 (2012) ("'Graymail' colloquially refers to situations where a defendant may seek to introduce tangentially related classified information solely to force the prosecution to dismiss the charges against him."); Hennessey & Weaver, *supra* note 8 (explaining that "graymail" is a situation where a "potential criminal defendant threatens to expose sensitive classified information if he is prosecuted" because the government "must choose between going forward with the prosecution, thereby compromising the classified material, or safeguarding the material but dropping the prosecution") (quoting Arjun Chandran, Note, *The Classified Information Procedures Act in the Age of Terrorism: Remodeling CIPA in an Offense-Specific Manner*, 64 DUKE L.J. 1411, 1415 (2015) (quoting *Graymail Legislation: Hearings Before the Subcomm. on Legis. of the H. Permanent Select Comm. on Intelligence*, 96th Cong. 1 (1979) (statement of Rep. Morgan Murphy, Chairman, Subcomm. on Legis. of the H. Permanent Select Comm. on Intelligence))).

18 *See* Joseph Cox, *Dozens of Lawyers Across the US Fight the FBI's Mass Hacking Campaign*, VICE: MOTHERBOARD (July 27, 2016, 12:15 PM), https://motherboard.vice.com/en_us/article/aek4ak/dozens-of-lawyers-across-the-us-fight-the-fbis-mass-hacking-campaign-playpen (describing the efforts of defense attorneys in the Playpen cases to coordinate their defense in a "national working group").

19 Ghappour, *supra* note 2, at 1079; *see also id.* at 1080 (explaining that this "new surveillance method [is] a practical solution for the pursuit of criminal suspects on the dark web").

how the government is able to hack into suspects' computers and deliver instructions telling the computer to relay identifying information to an FBI computer.[20] The stakes are high for the government because disclosing the code will render the NIT useless in future investigations;[21] potentially jeopardize other criminal investigations and intelligence operations using the NIT;[22] and may allow the NIT to be modified by malicious actors and used to hack into other systems.[23]

On the other hand, the intrusive nature of NITs is troubling because of the unbridled power they place in the government's hands. NITs allow investigators to take complete "control over a computer system"[24] without the owner's knowledge. As a result, the government may access more information than it represents in the warrant.[25] Additionally, flaws in NIT code can affect the integrity, or accuracy, of

---

[20] Hennessey & Weaver, *supra* note 8; *cf.* Cox, *supra* note 9 (describing how the NIT "grabbed targets' real IP address, MAC address, operating system and architecture, computer Host Name, and username" without using descriptive words such as "hacking" or "malware").

[21] *See* Kerr & Murphy, *supra* note 12, at 69 (noting that disclosure may "depriv[e] the government of future access to computers by using that same vulnerability"); Jennifer Granick & Riana Pfefferkorn, *Government Hacking: Evidence and Vulnerability Disclosure in Court*, CTR. FOR INTERNET & SOC'Y (May 23, 2017, 10:48 AM), http://cyberlaw.stanford.edu/blog/2017/05/government-hacking-evidence-and-vulnerability-disclosure-court ("[O]nce disclosed, the flaw will be patched and the government won't be able to use it reliably anymore."); *see, e.g.*, Nicholas Weaver, *The End of the NIT*, LAWFARE (Dec. 5, 2016, 2:30 PM), https://www.lawfareblog.com/end-nit (describing how the exposure of a NIT employed in another Dark Web investigation "effectively 'burned'" a subsequent investigation because "Mozilla deployed a patch within twelve hours, protecting . . . future NIT targets").

[22] *See* Gov't's Response to Defendant's Motion to Compel at 22, United States v. Darby, No. 2:16-cr-00036-RGD-DEM (E.D. Va. June 16, 2016), ECF No. 37 [hereinafter Darby Gov't's Response to Motion to Compel] (emphasizing that disclosure of the code could "discourage cooperation from third parties and other governmental agencies who rely on these techniques in critical situations"); Joseph Cox, *The Other Reason the FBI Doesn't Want to Reveal Its Hacking Techniques*, VICE: MOTHERBOARD (Mar. 30, 2016, 8:00 AM), https://motherboard.vice.com/en_us/article/yp3wgv/fbi-hacking-techniques ("[T]here is another reason the FBI doesn't want to reveal its techniques in court that isn't so obvious: The agency wants to avoid pissing off both its partners who provide the techniques, and other government agencies that might want to use those techniques for themselves.").

[23] *See* Weaver, *supra* note 21 (suggesting that malicious actors may "modify the exploit [(a component of the NIT code)] and use it to hack into other systems"); Jennifer Stisa Granick, *Challenging Government Hacking: What's at Stake*, ACLU (Nov. 2, 2017, 10:00 AM), https://www.aclu.org/blog/privacy-technology/internet-privacy/challenging-government-hacking-whats-stake ("Once a hacking tool has been disclosed outside the government, malicious actors have a window of opportunity to use it for their own nefarious purposes.").

[24] *See* Granick, *supra* note 23.

[25] *See id.* ("The FBI may have chosen to use that power only to collect identifying information, as it represented in the search warrant affidavit. But it could have accessed far more—and more private—information.").

data on the target computer or data transmitted to the FBI, and NITs may weaken computer systems, enabling unauthorized third parties to access them.[26] Defendants in the Playpen cases have argued that they must be able to review the entire NIT code to make independent determinations on these issues.[27] Commentators and the government, however, have argued that defendants do not need the *entire* NIT code to address their concerns; parts of the code suffice.[28] While criminal defendants have a right to information material to their defense,[29] it is unclear whether NIT code is material or simply tangentially relevant.[30]

In Jay Michaud's case, the defense convinced the court that it needed access to the full NIT code.[31] The judge conceded that the technical issues were over his head[32] but maintained that the code could be disclosed without compromising the government's inter-

---

[26] Granick & Pfefferkorn, *supra* note 21.

[27] *See, e.g.*, Defendant's Motion to Compel Discovery at 1, United States v. Darby, No. 2:16-cr-00036-RGD-DEM (E.D. Va. June 2, 2016), ECF No. 30 [hereinafter Darby Motion to Compel] (requesting "a copy of the code so that a computer forensics expert" can make independent determinations on the extent of information the government seized, whether the NIT affected any data or functions on the computer, and whether the government's representations are accurate).

[28] *See, e.g.*, Gov't's Response to Defendant's Motion to Compel at 5, 10, United States v. Anzalone, 221 F. Supp. 3d 189 (D. Mass. 2016) (No. 1:15-cr-10347-PBS), ECF No. 59 [hereinafter Anzalone Gov't's Response to Motion to Compel] (expressing the government's willingness to provide "the computer instructions that generated the identifying data, and the identifying data," and concern that the "defendant makes no showing as to how the NIT programming code, as opposed to other information that has been or could be made available, would actually further his defense"); Granick & Pfefferkorn, *supra* note 21 ("Playpen prosecutors also have argued . . . that it is sufficient for them to provide the payload information (IP address and other unique identity information) and data connecting the payload to the defendant's computer."); Hennessey & Weaver, *supra* note 8 (explaining that the "exploit" code in a NIT is not necessary to answer certain questions defendants and judges have about the government's use of a NIT).

[29] *See infra* Section II.A (discussing some of a defendant's rights in a criminal proceeding).

[30] This Note does not take a position on whether broadly speaking NIT code is material to a defendant's case. Determinations on materiality can vary on a case-by-case basis. *Compare* United States v. Matish, 193 F. Supp. 3d 585, 601 (E.D. Va. 2016) (finding that the full NIT code was not material), *with* Order on Procedural History and Case Status in Advance of May 25, 2016 Hearing at 2, United States v. Michaud, No. 3:15-cr-05351-RJB (W.D. Wash. May 18, 2016), ECF No. 205 [hereinafter Order on Procedural History] (finding that the defendant had proven that the full code was material).

[31] Order on Procedural History, *supra* note 30, at 2 ("[T]he defendant satisfied his threshold burden to show that the N.I.T. code would be material to his defense.").

[32] *Id.*; *see also* Newman, *supra* note 14 ("Judge Robert J. Bryan . . . noted that he did not have the technical expertise to evaluate any DoJ [sic] disclosure himself.").

ests.[33] The government disagreed and moved to dismiss the case.[34] This outcome is troubling because the judge's decision was based on incomplete information,[35] and the government likely had the evidence to prove its case beyond a reasonable doubt.[36] The case illustrates the difficulties new technologies pose for the criminal justice system. Although such cases are atypical, a single court's decisions can have broader ramifications for the government's use of NITs and the future of law enforcement.[37]

In criminal cases involving sensitive government information, courts must address an inherent tension between the government's legitimate interest in protecting sensitive information and defendants' constitutional and statutory rights. The FBI's use of law enforcement tools that exploit vulnerabilities, i.e., NITs, at large scales is new, and questions about how NITs should be treated procedurally are being litigated in court for the first time. This Note argues that courts must implement appropriate procedural safeguards to be able to make informed decisions on substantive issues regarding the disclosure of NIT code. If courts fail to do so, they may incentivize behavior antithetical to the pursuit of justice. Specifically: (1) the government may be forced to dismiss cases which can be proven beyond a reasonable doubt, (2) the defense may be encouraged to employ tactics that unnecessarily exhaust judicial resources, and (3) the government may turn to the trade secret privilege as a shield, effectively preventing defendants from accessing the code for law enforcement technology developed by third parties with a proprietary interest in the code.

The unique and complex nature of NITs as law enforcement tools merits exceptional procedural treatment. This Note proposes two pro-

---

[33] *See* Newman, *supra* note 14 ("Judge Robert J. Bryan suggested that the DOJ could use a protective order to give relevant details about the NIT to Michaud's defense in a limited and controlled way.").

[34] *See* Gov't's Unopposed Motion to Dismiss Indictment Without Prejudice, United States v. Michaud, No. 3:15-cr-05351-RJB (W.D. Wash. Mar. 17, 2017), ECF No. 227.

[35] *See* Gov't's Consol. Response to Defendant's Motion to Dismiss and Reply Regarding Motion for Reconsideration of Order Granting Defendant's Third Motion to Compel and for Leave to Submit Rule 16(d)(1) Filing *Ex Parte* and *In Camera* at 1–2, *Michaud*, No. 3:15-cr-05351-RJB (W.D. Wash. May 6, 2016), ECF No. 188 ("The government's previous decision to withdraw its request for [an ex parte and in camera] hearing was a misstep that left this Court with an incomplete picture on which to base its decision.").

[36] *See infra* notes 162–63 and accompanying text (noting that the government had seized the defendant's computers, hard drives, cell phones, and USB drives that all contained child pornography).

[37] *See infra* notes 128–29 and accompanying text.

cedural safeguards. Courts should hold ex parte[38] and in camera[39] proceedings[40] in order to understand the government's interests. Moreover, as law enforcement tools become more computer-based and technology plays a greater role in investigations, challenges to the government's use of technology will arise more frequently in court. Courts should hire their own experts to help judges grasp technical concepts relevant to the legal issues at hand. Courts must be prepared.

Much of the existing literature on NITs contemplates the validity of warrants that authorize the broad deployment of NITs and the legality of government hacking.[41] Other scholarship focuses on the international implications of U.S. law enforcement's use of NITs.[42] Yet discussions about the disclosure of NIT code in criminal proceedings are scarce,[43] even though the issue has compelled fierce litigation.[44] This Note focuses narrowly on the procedural safeguards courts should implement to ensure they receive sufficient information to appropriately weigh the government's interest in protecting NIT code against defendants' interest in disclosure. In doing so, it assumes that

---

[38] An ex parte proceeding is "[a] proceeding in which not all parties are present or given the opportunity to be heard." *Proceeding*, BLACK'S LAW DICTIONARY (10th ed. 2014).

[39] An in camera proceeding is "[a] proceeding held in a judge's chambers or other private place." *Id.*

[40] *See, e.g.*, *In re* City of New York, 607 F.3d 923, 948 (2d Cir. 2010) ("[F]iling documents under seal may inadequately protect particularly sensitive documents. . . . [T]he district court may, in the exercise of its informed discretion and on the basis of the circumstances presented, require that the party possessing the documents appear *ex parte* in chambers to submit the documents for *in camera* review . . . .").

[41] *See, e.g.*, 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, 30 (2016) (balancing the need for amendment of Rule 41 with concerns about the expansion of government power and proposing alterations); Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570, 580–81 (2018) (arguing that interpretation of Fourth Amendment doctrine dictates that government hacking is a search and "super-warrant procedures" should apply to government hacking); Brian L. Owsley, *Beware of Government Agents Bearing Trojan Horses*, 48 AKRON L. REV. 315, 318 (2015) (analyzing the validity of issuing search warrants for NITs).

[42] *See, e.g.*, Ghappour, *supra* note 2, at 1086 (arguing that "extraterritorial aspects of network investigative techniques demonstrate the need for new substantive and procedural regulations"); Kerr & Murphy, *supra* note 12 (critiquing Ghappour's article).

[43] For one example, see Christine W. Chen, Note, *The Graymail Problem Anew in a World Going Dark: Balancing the Interests of the Government and Defendants in Prosecutions Using Network Investigative Techniques (NITs)*, 19 COLUM. SCI. & TECH. L. REV. 185, 189 (2017) (arguing for the application of a heightened standard of relevance to request access to full NIT code and a general presumption that NIT code is not discoverable).

[44] *See* Cox, *supra* note 18 (describing defendants' calls for judges to suppress all evidence because the NIT warrant was unconstitutional or somehow flawed); Kerr, *supra* note 12 (noting that "district courts have handed down divided opinions on the legality of" the search warrant that authorized the Playpen NIT).

the government's evidence was lawfully obtained and poses no Fourth Amendment concerns.

The Note proceeds in three parts. Part I explains how NITs work and why they are invaluable surveillance tools for the government. Part II posits that courts struggle with NIT code discovery decisions because the technical issues are complex, and courts do not always have the information they need. Part II also addresses how courts' decisions on disclosure can negatively influence parties' practices. Part III concludes with recommendations for procedures courts can implement to improve their ability to employ existing balancing tests.

I
NITs in a Nutshell: The Value and Complexities of Network Investigative Techniques

The Internet is vast, and there are enormous parts that cannot be accessed by a Google search, including the notorious Dark Web which contains intentionally hidden content.[45] While journalists, political dissidents, and average individuals seeking privacy online use the Dark Web for legitimate purposes, its surreptitious nature has made it home to a wide range of illegal and dangerous activity.[46] The Dark Web can be accessed through various anonymizing services—the most popular being Tor.[47] Playpen was a hidden service that operated on the Tor network, and just one of hundreds of hidden websites dedicated to illicit activity including drug trafficking, money laundering, trade in stolen credit cards, trade in counterfeit currency, and pornography involving violence, children, and animals.[48] Criminals are readily using "the Internet to carry out traditional crimes" and facilitate tech-

[45] Kristin Finklea, Cong. Research Serv., R44101, Dark Web 2 (2017); Sui et al., *supra* note 1, at 6.

[46] Finklea, *supra* note 45, at 3. There is "a cast of anonymized Darknet operators whose activities are of enormous concern to government and to the public: drug dealers, hackers, hitmen, hoaxers, human traffickers, pimps, child pornographers, identity thieves, money launderers, leakers, political extremists, vigilantes, terrorists, and spies." Sui et al., *supra* note 1, at 10.

[47] Moore & Rid, *supra* note 1, at 15. Tor offers two services: anonymous browsing, and a network that hosts anonymous websites and services known as hidden services. *The Playpen Cases: Frequently Asked Questions*, Electronic Frontier Found., https://www.eff.org/pages/playpen-cases-frequently-asked-questions (last visited June 26, 2018). It requires downloading software that allows users to anonymously surf the web, and the Tor network "makes it possible for the software to work." *Id.* When users connect to websites through Tor, the website receives the IP address of a Tor exit relay after web traffic has been routed through several different servers so users' IP addresses remain anonymous. *Id.* Tor also allows the anonymous publication of websites and Internet services on the Tor network which can only be accessed through Tor. *Id.*

[48] Moore & Rid, *supra* note 1, at 20–25 (summarizing the results of a study that scanned sites on the Tor network).

nology-driven crimes, and "[t]he FBI considers high-tech crimes to be among the most significant crimes confronting the United States."[49]

NITs help the FBI locate criminals who hide their identities online through the use of services like Tor. Recently, law enforcement use of NITs has drawn broad public attention following multiple sting operations that took down hidden child pornography websites.[50] Part I describes NITs in depth and chronicles the FBI's use of NITs.

A. NITs Exploit Vulnerabilities

A network investigative technique[51] is software that overrides the security features that control access to computers.[52] NITs are essentially "exploit[s] or malware engineered to take advantage of a specific technology vulnerability."[53] While vulnerabilities can exist in hardware or software, "[s]oftware vulnerabilities are flaws or features in code that allow a third party to manipulate the computer running [the] software."[54] In this way, NITs allow the government to access and control targeted computers and retrieve their identifying information, such as a computer's IP address, by exploiting technological vulnerabilities.[55]

The efficacy of a NIT depends on the vulnerability it exploits. Not all technological vulnerabilities "are created equal—some are easier to find than others and only a small number will provide easy access to the best-secured software."[56] As a result, vulnerabilities are highly

---

[49] FINKLEA, *supra* note 45, at 9; Ghappour, *supra* note 2, at 1090 ("Increasingly, criminals use the dark web to facilitate crimes traditionally conducted in the physical world, such as currency counterfeiting, drug distribution, child exploitation, human trafficking, arms and ammunition sales, assassinations, and terrorism.").

[50] *See* 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/ (describing three major FBI sting operations since 2012).

[51] The term "network investigative technique" is a generic term the government uses; it "has no clear technical meaning." Kerr & Murphy, *supra* note 12, at 59 n.7.

[52] *See id.*

[53] KRISTIN FINKLEA, CONG. RESEARCH SERV., R44827, LAW ENFORCEMENT USING AND DISCLOSING TECHNOLOGY VULNERABILITIES 1 (2017). "Exploit" refers to "software, malware, or commands that can be used to take advantage of vulnerabilities in technology." *Id.*

[54] TREY HERR ET AL., BELFER CTR., TAKING STOCK: ESTIMATING VULNERABILITY REDISCOVERY 3 (2017).

[55] For example, the NIT used in the Playpen investigation is believed to exploit a vulnerability in Mozilla's Firefox browser code because the Tor browser is based on Firefox. Joseph Cox, *The FBI May Be Sitting on a Firefox Vulnerability*, VICE: MOTHERBOARD (Apr. 13, 2016, 2:25 PM), https://motherboard.vice.com/en_us/article/aekeq4/the-fbi-may-be-sitting-on-a-firefox-vulnerability.

[56] HERR ET AL., *supra* note 54, at 4.

coveted information;[57] unpatched and undisclosed, software vulnerabilities may be exploited by anyone who discovers them, and provide an entry point into computers running the flawed software.[58] A party who discovers one has no guarantee of being the only one who knows it exists, and the odds that another entity discovers it increase every day.[59] When vulnerabilities are disclosed or rediscovered, software makers and antivirus vendors act quickly to fix the flaw.[60] As a result, law enforcement must detect or acquire and rely on technology vulnerabilities that have not been patched or discovered by others.[61] This is extremely costly: Vulnerabilities can cost upwards of $100,000,[62] and even then the FBI does not always have the capabilities to develop exploits.[63] Thus vulnerabilities have a limited shelf life as NITs will become inoperative after the vulnerability is disclosed and repaired.

B. NITs Identify Criminals

Recently, the FBI has used NITs that rely on software vulnerabilities in Tor to identify anonymous individuals online.[64] These NITs "circumvent the operation of Tor to determine genuine IP addresses," and lead investigators to a user's Internet service provider (ISP) and physical location.[65] A NIT is comprised of four components, each of which plays a unique role in relaying the NIT to a target computer and

---

[57] Programmers and developers have a strong interest in vulnerabilities because they want to "discover the flaws in their code" and fix them. *Id.* at 2. "Bug bounties" have become a popular way for companies to learn about vulnerabilities, *id.*, but malicious actors will usually pay more for a vulnerability than the original developer. *Id.* at 4. This competition has created a growing market for buying and selling vulnerabilities "among criminal groups, companies, and governments." *Id.*

[58] *Id.* at 2.

[59] *Id.* at 4; Nicholas Weaver, *The FBI's Firefox Exploit*, LAWFARE (Apr. 7, 2016, 8:43 AM), https://www.lawfareblog.com/fbis-firefox-exploit ("It would be reasonable to assume Chinese or Russian hackers might discover the same weakness.").

[60] *See* Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1, 41 (explaining that software companies have "accelerated the rate at which they release security patches after critical vulnerabilities have been announced").

[61] There are policy debates on whether the government should disclose vulnerabilities. FINKLEA, *supra* note 53, at 1. The Obama Administration established the Vulnerabilities Equities Process (VEP) to help government agencies decide if they should disclose information about vulnerabilities they have acquired. *Id.* at 6. The process balances the intelligence and law enforcement value of the vulnerability against the public interest in disclosure. *Id.* at 7–8.

[62] Bellovin et al., *supra* note 60, at 42–43; Weaver, *supra* note 21.

[63] *See* Cox, *supra* note 22 (citing Christopher Soghoian, principal technologist at the ACLU, as stating that, "what's clear is that the FBI does not have the in-house capability to develop exploits").

[64] *See* FINKLEA, *supra* note 53, at 2.

[65] Hennessey & Weaver, *supra* note 8.

retrieving identifying information: (1) a generator, (2) the exploit, (3) the payload, and (4) a logging server.[66] The *generator* runs on a hidden service: It creates a unique ID to associate with a website visitor, and delivers that ID along with the exploit and payload to the website visitor's computer.[67] The generator allows the FBI to track specific NIT deployments to a computer.[68] After the generator transmits components of the NIT to the website visitor's computer, the *exploit*—the actual code that takes advantage of a vulnerability to gain control of a computer system[69]—takes control of the computer's Tor browser to load and execute the payload.[70] The *payload* program runs on the target computer, searches for authorized information, and transmits it to the logging service running on an FBI computer.[71] The *logging service* records the information collected from the computer, the ID assigned by the generator, and the computer's IP address.[72]

Once the FBI acquires information from a NIT, it can effectively use traditional investigative techniques to locate individuals. Typically, a computer's IP address, assigned by an ISP, reveals its location.[73] Using publicly available data, the FBI can identify the ISP that owns a computer's IP address.[74] The FBI then serves an administrative subpoena on the ISP to learn the name and address of the customer linked to the IP address.[75] This allows investigators to conduct surveillance of target premises and obtain appropriate search warrants.[76] But an IP address alone is not always sufficient to identify a criminal.[77] Consider Aaron McGrath, who was hosting three child pornography

---

66 *Id.*

67 *Id.*

68 *Id.*

69 *The Playpen Cases: Frequently Asked Questions*, *supra* note 47.

70 Hennessey & Weaver, *supra* note 8.

71 *Id.*

72 *Id.* The logging service specifically employs "packet capture," which produces "pcap" files to record network traffic as information is transmitted from the payload to the logging service. *Id.*

73 Erin Larson, *Tracking Criminals with Internet Protocol Addresses: Is Law Enforcement Correctly Identifying Perpetrators?*, 18 N.C. J.L. & TECH. 316, 317 (2017); Hennessey & Weaver, *supra* note 8.

74 *See, e.g.*, Application and Affidavit of Special Agent Jeffrey Tarpinian at 23, *In re* the Search of Computs. that Access the Website "Bulletin Board A," No. 8:12-MJ-356 (D. Neb. Nov. 16, 2012) [hereinafter Tarpinian Affidavit].

75 Hennessey & Weaver, *supra* note 8.

76 *Id.*; *see, e.g.*, Tarpinian Affidavit, *supra* note 74, at 24 ("The FBI has conducted surveillance of 510 Piedmont Dr., Omaha, NE, 68154, during the past 30 days.").

77 *See* Larson, *supra* note 73, at 319 (explaining that when law enforcement agents obtain an IP address, the IP address is "analogous to locating the phone tower that a cell phone connected to, rather than the actual phone used").

websites: one from his home and two from work.[78] The IP address associated with the site hosted from his home had been assigned to the woman with whom he lived.[79] It was only through physical surveillance of the home, searches of social media accounts, pen registers, and trap and trace orders,[80] and execution of search warrants that the FBI was able to hone in on McGrath.[81]

The FBI has expressed a firm belief that NITs are the only investigative technique "with a reasonable likelihood of securing the evidence necessary to prove beyond a reasonable doubt the actual location and identity" of individuals using anonymizing services to engage in federal offenses.[82] What identifying information does a NIT send the government? Since IP addresses are not reliable leads alone, a NIT identifies more than a target computer's IP address, but only enough to ensure that the FBI has identified the correct individual. The FBI's use of NITs in the various child pornography operations demonstrates how it has refined its techniques over time and is now able to collect more specific identifying information for an accurate match.

For example, the NIT used in Operation Torpedo, discussed below, acquired: the computer's IP address; the date and time the NIT determined the IP address; the "unique session identifier" that a website normally assigns to a visiting computer; and the type of operating system running on the computer.[83] The FBI explained why each piece of information was necessary: The IP address could be associated with an ISP and ISP customer, the session identifier would distinguish one computer's data from another, and the operating system details would help distinguish the targeted computer from other computers in the same premises.[84]

---

[78] 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/.

[79] *See* Tarpinian Affidavit, *supra* note 74, at 24 (noting that the IP address was assigned to Cox Internet customer Tiffany Strasser).

[80] Pen registers are devices that record the phone numbers that a particular phone number called. 18 U.S.C. § 3127(3) (2012). Trap and trace devices record the incoming phone numbers to a particular phone line. *Id.* § 3127(4).

[81] *See* Tarpinian Affidavit, *supra* note 74, at 25–29 (describing how the FBI connected Aaron McGrath to three hidden child pornography websites).

[82] *Id.* at 30. He added that "[d]ue to the unique nature of the Tor network and the method by which [it] protects the anonymity of its users by routing communications through multiple other computers or 'nodes,' . . . other investigative procedures that are usually employed in criminal investigations . . . have failed or reasonably appear to be unlikely to succeed." *Id.*

[83] *Id.* at 31.

[84] *Id.* at 31–32.

The Playpen NIT collected slightly more information. In addition to collecting the same information described above, the Playpen NIT obtained information about whether the NIT had been delivered to the computer, the computer's host name, the computer's active operating system username, and the computer's MAC address.[85] The host name served to "identify the device in various forms of electronic communication, such as communications over the Internet."[86] And the MAC address, which identified the network adapter connecting a computer to a network, allowed the FBI to determine whether suspects used the same adapter.[87]

C. The Government's Evolving Use of NITs

Given the increasing sophistication of anonymizing services, the inevitable rise and fall of vulnerabilities, and the limited investigatory value of an IP address, it should come as no surprise that government hacking has substantially evolved over the last two decades.[88] Not only has the government employed different types of NITs, which have exploited different vulnerabilities, but NITs have also progressively collected more detailed information to ensure that the FBI has apprehended the right person.[89] NITs are critical to criminal investigations—beyond those targeting hidden child pornography websites—and intelligence operations.

One of the earliest forms of the NIT as we know it is likely a surveillance tool called CIPAV, Computer and Internet Protocol Address Verifier, which came to light in 2009.[90] The tool has been

---

[85] Application & Affidavit of Special Agent Douglas McFarlane for a Search Warrant at 25, *In re* the Search of Comput. that Access upf45jv3bziuctml.onion, No. 1:15-SW-89 (E.D. Va. Feb. 20, 2015).

[86] *Id.*

[87] *Id.* at 25–26.

[88] It has been reported that the first known instance of government hacking involved the use of a keystroke logger, a program that records keystrokes entered on a computer keyboard, in 1999. *See* FINKLEA, *supra* note 53, at 2. The FBI was targeting Cosa Nostra mob boss Nicodemo Salvatore Scarfo, Jr., who was encrypting his communications. Zetter, *supra* note 50. They installed a keylogger on his computer to capture his encryption key. *Id.* Late in 2001, the FBI's use of Magic Lantern, an advanced keylogger that could be installed remotely, came to light. *Id.*

[89] *See* Poulsen, *supra* note 78 ("[A]n NIT can be a bulky full-featured backdoor program that gives the government access to your files, location, web history and webcam for a month at a time, or a slim, fleeting wisp of code that sends the FBI your computer's name and address, and then evaporates.").

[90] *See* Zetter, *supra* note 50 (describing the government's use of the Computer Internet Protocol Address Verifier (CIPAV)). CIPAV collects "a computer's IP and MAC address, an inventory of all open ports and software installed on the machine, as well as registry information, the username of anyone logged in and the last URL visited by the machine," and relays it to the FBI. *Id.*

used in numerous investigations on extortionists, hackers, terrorists, and foreign spies to "unmask[ ] the IP address of targets who used anonymizing services to hide their identity and location."[91] CIPAV was notably used in 2007 to identify a teenager sending bomb threats to a high school in Washington.[92] In less than two weeks, Timberline High School received nine anonymous threats that prompted evacuations and police sweeps, school administrators received menacing emails, and students were threatened from a social network account.[93] FBI agents sent a bugged link to the social network account and the suspect clicked the link, which allowed CIPAV to infiltrate his computer.[94] FBI agents linked the IP address they acquired with a Comcast account, and within a few hours a SWAT team raided the suspect's home; he was a student at the high school.[95]

To tackle the epidemic presence of child pornography on the Dark Web, the FBI has employed NITs in "watering hole attacks"[96] that target multiple people instead of singular targets. The FBI has used three different such NITs: in Operation Torpedo (2012); in an operation against the anonymous web hosting service, Freedom Hosting (2013); and in Operation Pacifier (2015).[97] Operation Torpedo took down three child pornography websites, including "Pedoboard,"[98] and the Freedom Hosting operation also attempted to target child pornography sites.[99] Operation Pacifier took down Playpen, a site with about 215,000 members.[100] It has identified thirty-five child sexual offenders, at least seventeen of whom were also producers of child pornography, and identified twenty-six child victims.[101] The NITs employed in the 2012 and 2013 operations were both compromised because components of the NIT code were publicly disclosed.[102] The Playpen NIT required the government to acquire a new

---

91 *Id.*

92 *Id.*; *see* Mayer, *supra* note 41, at 574–75 (providing an account of the FBI's investigation).

93 Mayer, *supra* note 41, at 574.

94 *Id.* at 575.

95 *Id.*

96 Watering hole attacks involve "embedding spyware on a website where criminal suspects congregate so computers of all visitors of the site get infected." Zetter, *supra* note 50.

97 *See* FINKLEA, *supra* note 53, at 4; Zetter, *supra* note 50.

98 Poulsen, *supra* note 78.

99 Zetter, *supra* note 50.

100 FINKLEA, *supra* note 53, at 4.

101 Hennessey & Weaver, *supra* note 8.

102 The vulnerability and exploit that the Torpedo NIT relied on was disclosed in *United States v. Cottom*. Memorandum and Order at 5–6, 15, United States v. Cottom, No. 8:15-cr-00239 (D. Neb. Dec. 22, 2015), 2015 WL 9308226 (describing FBI Special Agent Steven Smith's testimony on the NIT exploit and compiled code that the defense experts

vulnerability and develop a new exploit. Beyond criminal investigations, it has been speculated that NITs are being used in the national security context.[103] This should come as no surprise considering that the FBI has sought approval from the Foreign Intelligence Surveillance Court to use CIPAV in terrorism and espionage cases.[104] The FBI has also moved to classify the Playpen NIT code, citing national security reasons.[105]

In the last decade, government hacking has evolved and expanded in scope in an effort to keep up with cybercrime. The FBI's use of NITs in large sting operations is unprecedented, but the government must be able to investigate sophisticated criminals operating on the opaque Dark Web. As one court noted, "[l]aw enforcement cannot afford to be hamstrung by technologically creative criminals."[106] Part I endeavored to explain how NITs are unique as a law enforcement tool. They exploit technological vulnerabilities and perish upon public disclosure. Their value lies in their secrecy. Yet as the government pursues criminal charges against individuals identified in its child pornography stings, NITs have come under fire in courts across the country. There is an inherent tension between the government's interest in protecting the secrecy of NITs and defendants' due process rights.

II
NITs in Disarray: Shortcomings in Courts' Understanding of NITs

Operation Pacifier allowed the FBI to collect troves of incriminating evidence against many defendants charged with child exploitation and child pornography offenses. In response, zealous defense attorneys have challenged the FBI's use of NITs, and have asked the

examined). The NIT exploit used in the Freedom Hosting operation was discovered by Tor users who noticed "Javascript code that used a Firefox vulnerability to execute instructions on the victim's computer." Poulsen, *supra* note 78. Researchers used the exploit code to discover the vulnerability of which it took advantage. *Id.*

103 *See* Cox, *supra* note 22 (mentioning that the NIT may be used by other agencies including the NSA).

104 *See* Kevin Poulsen, *FBI's Sought Approval for Custom Spyware in FISA Court*, Wired (Feb. 6, 2008 12:27 PM), https://www.wired.com/2008/02/secretive-surve/#previouspost.

105 Joseph Cox, *The FBI Is Classifying Its Tor Browser Exploit Because 'National Security'*, Vice: Motherboard (June 24, 2016, 8:45 AM), https://motherboard.vice.com/en_us/article/gv5jwj/the-fbi-is-classifying-its-tor-browser-exploit (explaining that the FBI has classified portions of NIT code and deemed it sensitive government information that may only be accessed by those with the appropriate security clearance).

106 United States v. Acevedo-Lemu, No. SACR 15-00137-CJC, 2016 WL 4208436, at *6 (C.D. Cal. Aug. 8, 2016).

government to turn over the full NIT code for their review. They recognize that legal issues surrounding the use of NITs in criminal investigations are unsettled and have taken to testing the waters.[107] Defense teams across the country have coordinated their arguments and pleadings, have observed how the government has responded, and have followed courts' decisions in anticipation.[108]

Part II identifies problems courts face when considering whether NIT code should be disclosed to the defense and brings to light information gaps in courts' understanding of NITs and the stakes of disclosure for the government. In doing so, Part II reviews defendants' interest in the disclosure of NIT code and the government's interest in maintaining secrecy. Courts understand the stakes for defendants: Certain disclosures from the government help ensure defendants receive a fair trial. However, the government's interests can be shrouded in mystery due to its unwillingness or inability to discuss certain issues, some pertaining to national security, in open court. Courts cannot understand the stakes of disclosing the entire NIT code if the government cannot convey pertinent information to them. Additionally, when dealing with highly technical information, important details can get lost in translation. If courts do not understand the equities at stake, they will be ill-equipped to make decisions regarding disclosure. As a result, court decisions may incentivize behavior that harms the criminal justice system.

A. The Defendant's Rights

The Constitution guarantees criminal defendants a fair trial and "a meaningful opportunity to present a complete defense."[109] Although the Supreme Court has stated that there is no constitutional right to discovery in criminal cases,[110] the Court has acknowledged that discovery "minimizes the risk that a judgment will be predicated on incomplete, misleading, or even deliberately fabricated testimony."[111] Federal Rule of Criminal Procedure 16 governs discovery in

---

[107] Legal advocacy organizations have published a 188-page guide for criminal defense attorneys. *See generally* ACLU ET AL., CHALLENGING GOVERNMENT HACKING IN CRIMINAL CASES 2 (2017) ("This guide seeks to educate defense attorneys about these highly intrusive surveillance techniques and to help them prepare a zealous defense on behalf of their clients against secretive and potentially unlawful hacking.").

[108] Cox, *supra* note 18; *see, e.g.*, Darby Motion to Compel, *supra* note 27, at 1 ("In a similar case . . . the government . . . stated its intent not to provide this data . . . . The defendant anticipates that the government will take a similar position.").

[109] Crane v. Kentucky, 476 U.S. 683, 690 (1986) (citing California v. Trombetta, 467 U.S. 479, 485 (1984)).

[110] Weatherford v. Bursey, 429 U.S. 545, 559 (1977).

[111] Taylor v. Illinois, 484 U.S. 400, 411–12 (1988).

criminal proceedings and is rooted in the notion that "broad discovery contributes to the fair and efficient administration of criminal justice."[112] Under Rule 16, criminal defendants may request documents, information, and other tangible items if they are "within the government's possession, custody, or control" and are "material to preparing the defense."[113] In 1996, the Court clarified that for the purposes of Rule 16, "'the defendant's defense' means the defendant's response to the Government's case in chief."[114]

The Court has also held that criminal defendants have a narrower right to discovery under the Due Process Clause. *Brady v. Maryland* requires the government to disclose any exculpatory and impeachment evidence when it is "material either to guilt or to punishment."[115] Specifically, evidence is material "if there is a reasonable probability that, had the evidence been disclosed . . . the result of the proceeding would have been different."[116] But "[t]he mere possibility that an item of undisclosed information might have helped the defense, or might have affected the outcome of the trial, does not establish 'materiality' in the constitutional sense."[117] While the government's discovery obligations under Rule 16 are broader than pursuant to *Brady*,[118] it is the defense who bears the burden of proving materiality.[119] However, circuit courts have articulated different thresholds for materiality under Rule 16.[120] Furthermore, the Sixth

---

112 FED. R. CRIM. P. 16 advisory committee's note to 1974 amendment (noting that broad discovery promotes "the fair and efficient administration of criminal justice by providing the defendant with enough information to make an informed decision as to plea; by minimizing the undesirable effect of surprise at the trial; and by otherwise contributing to an accurate determination of the issue of guilt or innocence").

113 FED. R. CRIM. P. 16 (a)(1)(E).

114 United States v. Armstrong, 517 U.S. 456, 462 (1996).

115 373 U.S. 83, 87 (1963).

116 United States v. Bagley, 473 U.S. 667, 682 (1985). The court specified that "[a] 'reasonable probability' is a probability sufficient to undermine confidence in the outcome." *Id.*

117 United States v. Agurs, 427 U.S. 97, 109–10 (1976).

118 *See* United States v. Caro, 597 F.3d 608, 620 (4th Cir. 2010) ("Rule 16 differs from *Brady*, which rests upon due process considerations, and provides the minimum amount of pretrial discovery granted in criminal cases."); United States v. Baker, 453 F.3d 419, 424 (7th Cir. 2006) ("Rule 16 . . . is broader than *Brady*."); United States v. Conder, 423 F.2d 904, 911 (6th Cir. 1970) ("We are . . . of the view that the disclosure required by Rule 16 is much broader than that required by the due process standards of *Brady*.").

119 *See, e.g.*, *Caro*, 597 F.3d at 621 (noting that the defendant had to demonstrate materiality).

120 The Ninth Circuit has stated that "a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense," but that "neither a general description of the information sought nor conclusory allegations of materiality suffice." United States v. Mandel, 914 F.2d 1215, 1219 (9th Cir. 1990). The Fourth Circuit's test seems more rigorous: To show materiality under Rule 16(a)(1)(E)(i), "[t]here must be some indication that the pretrial disclosure of the disputed evidence

Amendment protects a defendant's right "to be confronted with the witnesses against him."[121]

Defendants have generally sought to acquire the full NIT code pursuant to Rule 16 and "fundamental notions of due process."[122] Specifically, defendants have sought the full code in order to "independently determine the full extent of the information seized by the government"; determine "whether the NIT interfered with or compromised any data or computer functions"; determine if the government is accurately representing how NITs work in warrant applications; and to establish the electronic "chain of custody" for the data that the NIT acquired.[123] These arguments are based on legitimate concerns. The FBI's use of the NIT could exceed the scope of a warrant by collecting more information than authorized.[124] The NIT code could simply contain flaws that affected the data that the FBI received.[125] The NIT could have tampered with data on the target computer. And the NIT could have left the target computer vulnerable to third parties who planted the child pornography evidence.[126] But these concerns beg the

---

would have enabled the defendant to significantly alter the quantum of proof in his favor." *Caro*, 597 F.3d at 621 (quoting United States v. Ross, 511 F.2d 757, 763 (5th Cir. 1975)). The D.C. Circuit has articulated that evidence is material when "there is a strong indication that it will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal." United States v. Lloyd, 992 F.2d 348, 351 (D.C. Cir. 1993).

121 U.S. CONST. amend. VI. Courts have recognized defendants' rights under the Confrontation Clause in the Playpen cases. *See, e.g.*, United States v. Matish, 193 F. Supp. 3d 585, 601 (E.D. Va. 2016) ("This particular issue concerns the public interest in nondisclosure and Defendant's rights to put on a defense and to confront witnesses against him under the Sixth and Fourteenth Amendments.").

122 *See, e.g.*, Darby Motion to Compel, *supra* note 27, at 4.

123 Motion to Compel at 1–2, United States v. Anzalone, No. 1:15-cr-10347-PBS (D. Mass. May 17, 2016). In *United States v. Cottom*, the defendant argued that the government's expert testimony should be excluded from trial because without reviewing the code for the NIT, he could not determine whether the NIT satisfied the *Daubert* rule. 679 F. App'x 518, 521 (8th Cir. 2017). The district court determined that the "government's experts satisfied the prerequisites under *Daubert*" regardless. *Id.* at 522.

124 Granick, *supra* note 23; Granick & Pfefferkorn, *supra* note 21; Hennessey & Weaver, *supra* note 8. However, the Playpen was deployed more narrowly than the warrant authorized. *See* Kerr, *supra* note 12 ("Although the warrant says that the NIT can be installed when a user logs in to his account, the government apparently only installed the NIT when a logged-in user clicked on a link to access the 'Preteen Videos—Girls Hardcore' forum.").

125 Granick & Pfefferkorn, *supra* note 21 (discussing how errors in the exploit code or how the code was found could impact the quality and accuracy of collected data); Hennessey & Weaver, *supra* note 8 (discussing how the NIT's data collection is "self-validating" because issues with the code would produce mismatched data that can be observed from the data alone).

126 Granick & Pfefferkorn, *supra* note 21; Hennessey & Weaver, *supra* note 8 ("It strains belief, but if this is in fact the defense theory, than [sic] examination of the exploit is material to that claim.").

question of whether the government must disclose the *entire* NIT code. Could the code of specific components of the NIT suffice?

B. The Information Gap: The Government's Position

The government's interest in nondisclosure lies in the need to protect sensitive information. As explained in Part I, the fact that NITs exploit vulnerabilities makes them unique and valuable. The government has a strong interest in maintaining the confidentiality of the full NIT code primarily because the exploit component of the code would reveal how the government bypassed Tor's anonymizing feature and the vulnerability it exploited.[127] Disclosing the full NIT code, including the exploit code, even under a protective order,[128] can result in the vulnerability being patched.[129] This would render the NIT useless and the FBI would have to find a costly replacement to continue fighting cybercrime. Moreover, other portions of NIT code are also sensitive, and disclosure may allow criminals to find ways around the technique and discourage other government agencies, who also rely on the NIT, from cooperating with the FBI.[130] This last point is particularly concerning because of the national security implications of disclosure.[131] NITs can be "comprised of hundreds or thousands of lines of code, much of which is implicated in highly sensitive law enforcement, military, and intelligence activity."[132]

Given the sensitive and sometimes classified nature of the information involved, the government has asserted that the full NIT code is

---

127 *See supra* note 69 and accompanying text.

128 Federal Rule of Criminal Procedure 16 allows courts to issue protective orders. FED. R. CRIM. P. 16(d)(1). The government often seeks protective orders before making disclosures to defendants when the material it intends to produce includes sensitive law enforcement information. *See, e.g.*, Stipulated Motion for Entry of Discovery Protective Order at 2, United States v. Michaud, No. 3:15-cr-05351-RJB (W.D. Wash. Aug. 10, 2015) (limiting dissemination of protected material and requiring filings under seal). However, even disclosure under a protective order runs the risk of leaks. *See, e.g.*, *In re* City of New York, 607 F.3d 923, 937–39 (2d Cir. 2010) (describing instances where sensitive information filed under seal was leaked to the public).

129 *See, e.g.*, Granick & Pfefferkorn, *supra* note 21 (noting that vulnerabilities are patched once they are disclosed).

130 Darby Gov't's Response to Motion to Compel, *supra* note 22, at 22.

131 *Id.* (noting that disclosure could "lead to other harmful consequences not suitable for inclusion in this response").

132 Hennessey & Weaver, *supra* note 8. According to a former deputy director of the NSA, "[c]omputer network exploitation tools are used every day to protect U.S. and allied forces in war zones, to identify threats to Americans overseas, and to isolate and disrupt terrorist plots." Rick Ledgett, *No, the U.S. Government Should Not Disclose All Vulnerabilities in Its Possession*, LAWFARE (Aug. 7, 2017, 8:30 AM), https://www.lawfareblog.com/no-us-government-should-not-disclose-all-vulnerabilities-its-possession.

protected by a law enforcement privilege.[133] The government has also requested ex parte and in camera proceedings to explain their privilege claim, but is not always granted them.[134] While the government has compelling reasons to withhold the entire NIT code from disclosure, these explanations are worthless if courts do not hear them. The parties in *United States v. Michaud*[135] were among the first to wrestle with legal issues surrounding NIT code, and the case illustrates the challenges they pose for courts.

The court reached contradictory conclusions, ruling that Michaud had the right to review the full NIT code because it was material to his defense and then finding that the government was not required to produce the information.[136] Two shortcomings during the proceedings contributed to the problem: (1) important technical information about the NIT was lost on the court, and (2) the court did not receive the information necessary to understand the stakes for the government because it did not hold a timely ex parte in camera hearing.

First, as the government and the defense wrestled over what information prosecutors were required to produce, the technical details about components of the NIT code and their potential evidentiary value were lost on the court. When the defense sought to compel discovery of the full NIT code,[137] the government maintained that it was protected by a qualified law enforcement privilege—disclosure would compromise ongoing investigations and harm the public interest.[138] Instead, the government offered the defense an opportunity to review "the *instructions* sent to [Michaud]'s computer . . . that produced the NIT results" at an FBI facility.[139] To be clear, the computer instructions do not comprise the entire NIT code; they explain what commands the NIT forced the computer to execute so it would relay identifying information to the FBI. Due to a misunderstanding,

---

133 The government has asserted that the full NIT code is subject to the qualified law enforcement privilege in numerous Playpen cases. *See, e.g.*, United States v. Matish, 193 F. Supp. 3d 585, 600 (E.D. Va. 2016); Darby Gov't's Response to Motion to Compel, *supra* note 22, at 2; *see also infra* Part III.

134 *See, e.g.*, U.S.' Response to Defendant's Motion to Compel at 13, United States v. Michaud, No. 3:15-cr-05351-RJB (W.D. Wash. Jan. 21, 2016) [hereinafter Michaud Gov't's Response to Third Motion to Compel] (requesting an ex parte and in camera hearing).

135 No. 3:15-cr-05351-RJB, 2016 BL 25171 (W.D. Wash. Jan. 28, 2016).

136 Order on Procedural History, *supra* note 30, at 2–3.

137 *Id.* at 2.

138 *See* U.S.' Response to Defendant's Motion to Compel at 15, *Michaud*, No. 3:15-cr-05351-RJB (W.D. Wash. Dec. 4, 2015), ECF No. 74 [hereinafter Michaud Gov't's Response to First Motion to Compel] (stating that the NIT code is "subject to a qualified law enforcement privilege, as its disclosure would be harmful to the public interest").

139 Michaud Gov't's Response to Third Motion to Compel, *supra* note 134, at 4 (emphasis added).

the defense withdrew its request to compel the full NIT code.[140] In January 2016, when the defense received discovery and realized the full NIT code was missing, it commenced another motion to compel.[141]

In response, the government rehashed many of the same arguments from its earlier response.[142] The government stressed that it had provided "substantial discovery,"[143] and explained that the full NIT code was not necessary for the independent review that the defense's expert intended to conduct.[144] In other words, the government insisted that a review of the information it had already disclosed would allow the defense to resolve its questions.[145] These details—understanding the technical components of the NIT and value of information that had already been produced—were important to evaluating the potential evidentiary value of the full NIT code, but the court failed to appreciate the details.

This became clear during the hearing on the motion to compel discovery and in one of Judge Bryan's orders. After concluding that the full NIT code was material, Judge Bryan stated, "Much of the details of this information is lost on me, I am afraid, the technical parts of it . . . this whole thing didn't seem that complex to me."[146] He did not consider the materiality of the parts of the code as opposed to the whole code. Furthermore, it is worth noting that the judge's order, which summarized the "protracted discovery battle between the parties," only referred to the NIT code in its entirety and did not acknowledge the information and parts of the NIT code that the gov-

---

140 *See* Order on Procedural History, *supra* note 30, at 2 (noting that "the defendant had withdrawn his request to compel the N.I.T. code").

141 *See* Third Motion and Memorandum of Law in Support of Motion to Compel Discovery at 3, *Michaud*, No. 3:15-cr-05351-RJB (W.D. Wash. Jan. 14, 2016), ECF No. 115 (noting that the defense's code expert noticed that the data from the government was incomplete).

142 *Compare* Michaud Gov't's Response to Third Motion to Compel, *supra* note 134, *with* Michaud Gov't's Response to First Motion to Compel, *supra* note 138.

143 Michaud Gov't's Response to Third Motion to Compel, *supra* note 134, at 1 ("The information provided included . . . a copy of the computer instructions . . . [that] produced the NIT results, the NIT results themselves, the date and time . . . [of] execut[ion] . . . , the Website A page that Michaud was accessing when the NIT was executed, and access to computers and digital devices that were seized . . . .").

144 *See id.* at 8–12 (explaining how different information the government produced answered the questions that Michaud claimed required the full code to do so).

145 *See* Darby Gov't's Response to Motion to Compel, *supra* note 22, at 29 ("[T]he defendant has been provided or has access through discovery to 'adequate alternative means of getting at the same point' to which he claims disclosure of information is relevant." (citing United States v. Harley, 682 F.2d 1018, 1020 (D.C. Cir. 1982))).

146 Transcript of Motion Hearing at 18–19, *Michaud*, No. 3:15-cr-05351-RJB (W.D. Wash. Feb. 17, 2016), ECF No. 162.

ernment had produced.[147] NIT code has been widely discussed in reference to its components,[148] e.g., the exploit code, and it is unclear whether Judge Bryan considered these key subtleties. In contrast, the court in *United States v. Matish* parsed out the NIT code and explicitly considered whether the defense required the NIT exploit code.[149] Judge Bryan never acknowledged the exploit code.

Second, the failure to hold an ex parte and in camera proceeding on the government's law enforcement privilege prior to the hearing on the motion to compel prevented the court from receiving information necessary to make an informed decision. At the hearing, the court, relying solely on the government's public filings, stated, "[W]hat has been presented is nothing more than a showing that disclosure could possibly lead to harmful consequences. I think that is not sufficient to justify a separate hearing . . . . It is my opinion that the protective order in place is sufficient to protect this information."[150] The court denied the government's request for a closed hearing, and as a result, did not fully grasp the government's interest in nondisclosure. Months after the court granted Michaud's request for the full NIT code, the court held the ex parte in camera hearing at the government's behest and ruled that the government was not required to disclose the code. The NIT code was not classified, but the reason for nondisclosure was.[151] At the same time, the court affirmed the full NIT code's materiality and Michaud's right to review it:[152] the epitome of a catch-22 that resulted in the government dismissing the indictment.[153] Again, it is worth comparing with *Matish*. The court in *Matish* did not hold an ex parte and in camera hearing for a very different reason: The court

147 Order on Procedural History, *supra* note 30, at 1.

148 *See* Declaration of Vlad Tsyrklevich at 2–3, *Michaud*, No. 3:15-cr-05351-RJB (W.D. Wash. Jan. 13, 2016), ECF No. 115-1 (describing the components of the NIT that the government did not disclose); Hennessey & Weaver, *supra* note 8 (same); Weaver, *supra* note 21 (same).

149 193 F. Supp. 3d 585, 600 (E.D. Va. 2016) (concluding that the defense had failed show that the exploit "will play an important role in uncovering admissible evidence, aiding witness preparation, corroboration testimony, or assisting impeachment or rebuttal" (quoting United States v. Caro, 597 F.3d 608, 621 (4th Cir. 2010))).

150 Transcript of Motion Hearing, *supra* note 146, at 17–18.

151 The defense noted that the government never argued that the NIT code was classified. However, the government was "relying on the classified nature of the information it want[ed] to present to persuade the Court to grant ex parte proceedings and vacate its discovery order." Reply to Gov't's Response to Second Defense Motion to Dismiss Indictment at 3, United States v. Michaud, No. 3:15-cr-05351-RJB (W.D. Wash. May 9, 2016), ECF No. 191.

152 *See* Order on Procedural History, *supra* note 30, at 5.

153 *See* Gov't's Unopposed Motion to Dismiss Indictment Without Prejudice, *Michaud*, No. 3:15-cr-05351-RJB (W.D. Wash. Mar. 3, 2017), ECF No. 227.

trusted the government.[154] However, such faith in the government is not necessarily warranted.[155]

Following the mishap in *Michaud*, the FBI learned its lesson. In *United States v. Darby*, another Playpen case, the government revealed that the FBI had "derivatively classified portions" of the NIT code.[156] The government requested an ex parte and in camera proceeding,[157] and two months later, the court denied the defendant's motion to compel discovery.[158] This narrative illustrates how the technical complexities of NITs can get lost in translation. Nevertheless, courts need to understand some technical details and know the risks disclosure of the full NIT code pose for the government to make an informed decision.

C. Repercussions

If courts make swift decisions about whether the full NIT code should be disclosed in criminal cases without grasping at least some of its intricacies and being aware of the government's stake in disclosure, it may incentivize behavior that harms the criminal justice system. Courts can err in two ways[159]: (1) Courts many rule that the defendant's need to access the entire NIT code outweighs the government's interest in confidentiality and order that it be disclosed, when in reality the entire code is not material to the defense, or (2) courts may rule that the government's interest in the confidentiality of the entire NIT code is greater than the defendant's need to review it and withhold disclosure when in reality, the code is material to the defense. If courts err on decisions of disclosure in the first instance, the government may be forced to dismiss cases that can be proven beyond a reasonable doubt in order to protect sensitive information that is only tangentially related to the government's case-in-chief. In numerous

---

154 *See Matish*, 193 F. Supp. 3d at 599–600 (finding an ex parte and in camera proceeding to be unnecessary). The court stated: "Such examination would not have assisted the Court in dealing with the issues before it. The technicalities of such an examination are better left to computer experts. The Court places its reliance on the declaration and testimony of SA Alfin." *Id.*

155 *See, e.g.*, Cyrus Farivar & Joe Mullin, *Stealing Bitcoins with Badges: How Silk Road's Dirty Cops Got Caught*, Ars Technica (Aug. 17, 2016, 6:00 AM), https://arstechnica.com/tech-policy/2016/08/stealing-bitcoins-with-badges-how-silk-roads-dirty-cops-got-caught/ (explaining how a DEA agent and a Secret Service agent investigating the Silk Road case were involved in digital currency theft).

156 Darby Gov't's Response to Motion to Compel, *supra* note 22, at 22 n.8.

157 *See id.* at 22.

158 *See* Opinion and Order, United States v. Darby, No. 2:16-cr-00036-RGD-DEM (E.D. Va. Aug. 12, 2016), ECF No. 49 [hereinafter Darby Opinion and Order].

159 When considering whether sensitive government information should be disclosed to criminal defendants, courts employ a balancing test discussed in detail in Section III.A.

Playpen cases, the government argued that it would not be using the NIT code in its case at trial,[160] and corroborating evidence has borne out a strong connection between defendants and the alleged criminal offenses. Although the Playpen NIT helped the FBI identify individuals who accessed the website, the most condemning evidence was obtained during the execution of search warrants at the premises where defendants accessed the website,[161] and in interviews.[162] The FBI seized computers, hard drives, cell phones, and USB drives containing child pornography.[163] The government's cases rested on *this incriminating evidence*.[164] Dismissal under these circumstances is troubling because potential criminal offenders may not be held accountable and their release can pose public safety concerns.

For example, during the search of Vincent Anzalone's home, a Playpen defendant, law enforcement agents seized three computers, a hard drive, and a smart phone, and Anzalone was interrogated.[165] During the interrogation, Anzalone allegedly admitted to possessing child pornography, having had sexual contact with a niece when he was 17, having had sex with potentially underage girls in Asia when he was in the Navy, and engaging in heavy petting with an underage

---

160 *See* Anzalone Gov't's Response to Motion to Compel, *supra* note 28, at 2 (noting that the government did not intend to use the NIT code in its case-in-chief at trial); Darby Gov't's Response to Motion to Compel, *supra* note 22, at 3 (same); Michaud Gov't's Response to Third Motion to Compel, *supra* note 134, at 7 ("[T]he only NIT information relied upon by the government in the warrant for Michaud's home and that it may rely on at trial is that which has already been disclosed.").

161 *See* Hennessey & Weaver, *supra* note 8 (noting that criminal charges were based on evidence obtained from NIT deployments and the execution of physical search warrants "authorized pursuant to NIT-based probable cause").

162 *See, e.g.*, United States v. Brooks, No. 16-CR-6028L, 2016 BL 428566, at *9 (W.D.N.Y. Dec. 22, 2016) (describing how an interview with the defendant led FBI agents to two USB drives in the sewer); Defendant's Memorandum in Support of Motion to Suppress at 15, United States v. Anzalone, No. 1:15-cr-10347-PBS (D. Mass. May 13, 2016), ECF No. 48 ("[A]gents seized three computers, a hard drive, and a smart phone. Anzalone was then detained and interrogated, during which he agreed to take a polygraph test.").

163 *See, e.g.*, *Brooks*, 2016 BL 428566, at *20 (noting that law enforcement agents found three USB drives).

164 These scenarios assume that the warrant authorizing the use of the NIT was valid, as many courts have found, and that the Playpen NIT was executed in a manner that does not implicate fruit of the poisonous tree concerns (e.g., the NIT code was not flawed, or the NIT did not access information beyond the scope of the search warrant). However, in cases of impermissible use of NITs, defendants' need to access the code will be greater than the government's interest in protecting it. The decision rests with courts and requires considering whether defendants must access the *entire* code to vindicate their claims. *See, e.g.*, Hennessey & Weaver, *supra* note 8 (noting that if defendants claim that NIT code contains programming errors, or that "an unknown third party planted or otherwise compromised evidence," they would not need to review the entire NIT code to address their concerns).

165 *See* Defendant's Memorandum in Support of Motion to Suppress, *supra* note 162, at 15.

girl.[166] Most of the events had occurred over ten years earlier and Anzalone had never been charged with a sex-related offense.[167] The FBI's use of the Playpen NIT was precursory, and evidence acquired later could stand on its own.[168]

Similarly in Michaud's case, information acquired from the NIT helped the FBI identify Playpen user "pewter."[169] It was the execution of a search warrant on Michaud's home that produced a cell phone and two thumb drives containing child pornography.[170] Even though the court found that the entire NIT code was material to the defense, there is a real chance that the court got it wrong.[171] Further, as mentioned earlier, the court ruled that disclosure under a protective order was sufficient to protect the government's interests; protective orders, however, have their shortcomings and pose risks that the government would reasonably want to avoid.[172] Unlike Anzalone and many others, Michaud's case was dismissed. He went back to his life, but was recently prosecuted for a child pornography offense by local prosecutors.[173] The fact remained: He certainly possessed child pornography.

Relatedly, defendants, having seen the successful outcome of requests to access the full NIT code, will feel emboldened to make similar claims in their own cases and "graymail" the government—a tactic where defendants try to introduce immaterial sensitive information into a case "solely to force the government to dismiss the

---

166 *Id.*

167 *Id.*

168 The evidence did stand on its own. Anzalone eventually entered into a plea agreement with the government. Plea Agreement, United States v. Anzalone, No. 1:15-cr-10347-PBS (D. Mass. Jan. 26, 2017), ECF No. 106.

169 Gov't's Motion for Reconsideration of Order Granting Defendant's Third Motion to Compel and for Leave to Submit Rule 16(d)(1) Filing Ex Parte and In Camera at 5, United States v. Michaud, No. 3:15-cr-05351-RJB (W.D. Wash. Mar. 29, 2016), ECF No. 168.

170 *Id.* at 5 (noting that the images had been "organized into folders by subject" and that the thumb drive had a "downloads" folder with "subfolders with names such as 'Little-Virgins' and 'Nasties' that contained child pornography").

171 Other courts have held that the full Playpen NIT code is not material to the defense. *See, e.g.*, Darby Opinion and Order, *supra* note 158, at 8 (explaining that the defendant did not establish materiality of the NIT code because the defendant "place[d] before the Court . . . stories about how a generic defendant located by means of a generic NIT might need the information sought" and did not "establish a factual basis for these scenarios"); United States v. Matish, 193 F. Supp. 3d 585, 598 (E.D. Va. 2016) ("Notably, the purposes for which Defendant asks for access to the missing source code are based upon speculation . . . . The defense lacks any evidence to support the hypotheses.").

172 *See infra* notes 252–55 and accompanying text.

173 *See* Jessica Prokop, *Ex-Teacher Faces Child Porn Charges Again*, COLUMBIAN (Apr. 17, 2018, 6:25 PM), http://www.columbian.com/news/2018/apr/17/ex-teacher-faces-child-porn-charges-again/.

charges."[174] This is a concern because it can distract from the criminal offense at issue and unnecessarily exhaust judicial resources through prolonged motion practice. Following the Playpen investigation, many defendants quickly pled guilty looking at the mountain of evidence against them.[175] Outcomes like *Michaud*, however, signaled that it was possible to get charges dropped if defense teams were creative enough and convinced courts that the full NIT was material to their defense. Defense teams were able to follow a playbook.[176] As a result, some defendants who had pled guilty successfully withdrew their pleas.[177]

Defendants undoubtedly have a right to discovery and to material information, and defense attorneys must be zealous advocates. It is, however, worth considering how many Playpen defendants seriously believed the FBI's NIT wrongfully identified them or that child pornography was planted on their electronics. Even though many defendants who have requested to access the full Playpen NIT code eventually plead guilty,[178] as proceedings have extended over time due to the NIT question they have consumed limited judicial resources.

Finally, the government, in order to avoid litigation over the disclosure of NIT code and protect the confidentiality of law enforcement technology, may begin shielding itself behind the "criminal trade secret privilege."[179] A trade secret is a "formula, process, device, or other business information that is kept confidential to maintain an advantage over competitors."[180] In civil litigation, trade secrets may

---

174 LIU & GARVEY, *supra* note 17, at 1.

175 *See* Cox, *supra* note 18.

176 The legal guide for defense attorneys litigating these issues contains an appendix with sample briefs to compel discovery of NIT code. ACLU ET AL., *supra* note 107, at 43–188. Actual requests for the full NIT code have relied on the same arguments and mirror language in the guide. *Compare id.* at 44 (exhibiting a motion to compel discovery of NIT code "so that a computer forensic expert can independently determine the full extent of the vulnerability created by the government . . . ; whether the NIT interfered with or compromised any data or computer functions; and whether the government's representations about how the exploit worked are complete and accurate"), *with* Darby Motion to Compel, *supra* note 27, at 1 (using identical language as the ACLU's motion).

177 *See* Cox, *supra* note 18.

178 *See, e.g.*, Plea Agreement, *supra* note 168; Plea Agreement, *United States v. Matish*, 4:16-cr-00016-HCM-RJK (E.D. Va. Oct. 18, 2016), ECF No. 93; Plea Agreement, *United States v. Darby*, No. 2:16-cr-00036-RGD-DEM (E.D. Va. Sept. 8, 2016), ECF No. 54.

179 *See* Rebecca Wexler, *Life, Liberty, and Trade Secrets*, 70 STAN. L. REV. 1343 (2018) (arguing that trade secrets should not be privileged in criminal proceedings).

180 *Trade Secret*, BLACK'S LAW DICTIONARY (10th ed. 2014). Additionally, the Uniform Trade Secrets Act defines a "trade secret" as "information . . . that: (i) derives independent economic value, actual or potential, from not being generally known to . . . other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy." UNIF. TRADE SECRETS ACT § 1(4) (amended 1985) (UNIF. LAW COMM'N 1986).

be protected during discovery through issuances of protective orders.[181] In criminal prosecutions, federal courts can take "action as may be necessary and appropriate to preserve the confidentiality of trade secrets."[182] The government cannot invoke the trade secret privilege in litigation; rather, it relies on the state secrets privilege in civil litigation,[183] and the Classified Information Procedures Act (CIPA)[184] in criminal cases to protect sensitive government information.[185]

As Rebecca Wexler notes, "emerging criminal justice technologies . . . are also, for the most part, privately owned," and "[d]evelopers often assert that details about how their tools function are trade secrets."[186] As a result, third parties that develop law enforcement technology have successfully asserted the trade secret privilege in criminal proceedings to prevent defendants from obtaining the code for their technology.[187] Alcohol breath testing devices and probabilistic genotyping software like TrueAllele are notorious examples.[188] In these cases, courts tend to cast aside issues concerning the accuracy and reliability of the technology,[189] and

---

181 *See* FED. R. CIV. P. 26(c)(1)(G).

182 18 U.S.C. § 1835 (2012).

183 *See* LIU & GARVEY, *supra* note 17, at 1 ("The state secrets privilege is a judicially created evidentiary privilege that allows the government to resist court-ordered disclosure of information during civil litigation, if there is a reasonable danger that such disclosure would harm the national security of the United States.").

184 18 U.S.C.A. app. 3 §§ 1–16 (West 2012).

185 *See* LIU & GARVEY, *supra* note 17, at 2.

186 Wexler, *supra* note 179, at 1349–50.

187 *See* Edward J. Imwinkelried, *Computer Source Code: A Source of the Growing Controversy over the Reliability of Automated Forensic Techniques*, 66 DEPAUL L. REV. 97, 100 & n.20 (2016) (noting that courts have denied defendants' request to access the source code for breath testing devices, an enhanced peer-to-peer file sharing program, EP2P, and probabilistic genotyping programs like TrueAllele); Wexler, *supra* note 179, at 1346 (describing how a "death penalty defendant . . . was denied access to the source code for a forensic software program that generated the critical evidence against him; the program's commercial vendor argued the code is a trade secret"); Colin Holloway, *Pennsylvania Judge Denies Access to Source Code Behind DNA Expert Witness Software*, EXPERT PAGES: BLOG (Feb. 6, 2016), https://blog.expertpages.com/expertwitness/pennsylvania-judge-denies-access-to-source-code-behind-dna-expert-witness-software.htm (noting that TrueAllele's creator, Mark Perlin, "has consistently resisted sharing his source code by arguing it would be economically disadvantageous for his company to do so"); *cf.* Aurora J. Wilson, *Discovery of Breathalyzer Source Code in DUI Prosecutions*, 7 WASH. J.L. TECH. & ARTS 121, 123 (2011) ("In *State v. Underdahl*, the Minnesota Supreme Court upheld an order compelling discovery of breathalyzer source code . . . .").

188 *See generally* Imwinkelried, *supra* note 187 at 98–99 (criticizing how forensic analysis is increasingly being computerized without sufficient care to accuracy and quality of the program's code); Natalie Ram, *Innovating Criminal Justice*, 112 NW. U. L. REV. 659, 660–61 (2018) (noting the growing use of the trade secret privilege to prevent the disclosure of source code for various law enforcement tools).

189 *See* Andrea Roth, *Machine Testimony*, 126 YALE L.J. 1972, 1978 (2017) (explaining that a machine's programming could produce false, imprecise, and ambiguous results

defendants' rights summarily take second chair to the blanket trade secret protection. Manufacturers of breath testing devices used to measure levels of intoxication in drivers have refused to allow criminal defense experts to review the code underlying the devices, asserting trade secrecy.[190] And these claims have prevailed[191] even though criminal defendants may have good reasons to request to examine the code: Intoxilyzer devices have been found to produce false positives for people who suffer from diabetes, and the Drager Alcotest 7110 had been found to lack critical error detecting functions.[192]

Even more alarming is the criminal justice system's treatment of probabilistic genotyping software, the most popular being TrueAllele, which has been used to convict defendants charged with serious crimes. Billy Ray Johnson was convicted for a series of sexual assaults and burglaries and handed a life sentence without parole because TrueAllele linked Johnson to traces of DNA found at multiple crime scenes.[193] The defense expert sought to examine TrueAllele's source code, but its creator Mark Perlin refused to disclose it, maintaining it was a trade secret.[194] The judge refused to order the disclosure of the source code, yet admitted TrueAllele's DNA analysis into evidence even though the investigators, prosecutors, defense attorneys, and the judge were not allowed to review the code.[195] Even though TrueAllele has been used in over 500 criminal cases,[196] courts have not ordered the discovery of the code and "no one outside of Cybergenetics—Perlin's company—has seen or examined that source code."[197] How-

"because of human error at the programming, input, or operation stage, or because of machine error due to degradation and environmental forces"); Wexler, *supra* note 179, at 1369–70 (suggesting that "a defendant's and a judge's incentives to scrutinize" risk assessments programs used at sentencing "might differ, or that only one chooses to rely on the system while blind to its methodology"); Christian Chessman, Note, *A "Source" of Error: Computer Code, Criminal Defendants, and the Constitution*, 105 CALIF. L. REV. 179, 184 (2017) (suggesting that "computer programs do not automatically or inherently enhance reliability of evidence" and that they are "susceptible to human manipulation"). For example, a review of the code of a breathalyzer machine, the Alcotest 7110, revealed that even though it was "'generally scientifically reliable,' its software had several 'mechanical and technical shortcomings.'" Roth, *supra*, at 1995.

190 *See* Ram, *supra* note 188, at 671–72.

191 *Id.* (explaining that courts have "repeatedly vindicated manufacturers' trade secret claims" by "acced[ing] to manufacturers' assertions of trade secret protection" or finding that the state does not possess the requested code and thus is not in a position to disclose it).

192 *Id.* at 674.

193 *Id.* at 660–61.

194 *Id.*

195 *Id.*

196 *See* Imwinkelried, *supra* note 187, at 100–01.

197 Ram, *supra* note 188, at 661.

ever, this criminal trade secret privilege is "not limited to any particular category of forensic technology"; for example, algorithms for latent fingerprint analysis are also proprietary, and as law enforcement techniques increasingly rely on proprietary technology, third parties will increasingly assert the trade secret privilege in criminal cases.[198] This is disconcerting for the future of law enforcement and the criminal justice system because it amounts to an unassailable bar on accessing the code for law enforcement technology when defendants have legitimate reasons for requesting the code.

The unabashed protection of third parties' interests is puzzling. Surely from a moral perspective, a defendant's right to acquire the code for law enforcement technology, whether it is breathalyzer technology, DNA software, or a NIT, cannot—and should not—hinge on a trade secret distinction.[199] It is contrary to an adversarial system of justice and absolves the government of its burden in criminal cases. Nevertheless, the trade secret privilege is viewed favorably in criminal proceedings,[200] and the government may very well decide to contract with a third party to develop future NITs. Imagine a future where all sophisticated law enforcement and surveillance technology is protected as a trade secret in criminal proceedings and cannot be disclosed to defendants because it belongs to third parties.

The government's potential reliance on the trade secret privilege to shield NIT code will depend on how the government acquires vulnerabilities and develops NITs. Vulnerabilities may be publicly available, discovered, or purchased from hackers on the vulnerabilities market.[201] Moreover, the government may develop its own exploits, purchase off-the-shelf exploits on the black market,[202] or "contract an outside entity to develop them."[203] The trade secret privilege may apply where a contractor is involved, where the government uses a NIT developed by a third party, or where it otherwise utilizes a third party's proprietary information in its NITs. Thus, the repercussions of courts' rulings on the disclosure of NIT code without understanding the government's stakes and the technicalities of NITs are real and troubling.

---

198 *See* Wexler, *supra* note 179, at 1363.

199 *See id.* 1353–55 (contending that trade secret privilege should not exist in criminal cases because it is unnecessary in light of narrow criminal discovery and it overprotects intellectual property compared to substantive trade secret law).

200 *Id.*

201 *See* FINKLEA, *supra* note 53, at 12; *see also* Bellovin et al., *supra* note 60, at 42 (noting that the vulnerabilities market is a "relatively recent phenomenon").

202 *See* Bellovin et al., *supra* note 60, at 39.

203 FINKLEA, *supra* note 53, at 12.

Part II identified two problems that arise when judges consider whether the government must disclose the entire NIT code to the defense. First, courts have turned down requests for ex parte and in camera hearings where the government can present the court with sensitive information pertinent to understanding the equities at stake. Second, courts struggle with technical details about NITs that are critical to their decisions on disclosure and materiality.

If courts rule on the government's obligation to disclose NIT code without being able to gauge the potential evidentiary value of the full code and knowing the stakes—and those courts get it wrong—it could force the government to dismiss cases against criminals who threaten public safety. It could embolden similarly situated defendants to extend pre-trial proceedings by making hollow claims to access the complete NIT code. This can distract from the criminal offense at issue and expend judicial resources. Finally, it could push the government to shield itself behind the trade secret privilege, closing the door to any considerations about disclosure.

III
NITs in Balance: Procedures for Courts to Better Evaluate NITs

In order to best equip courts to decide on the evidentiary value of NIT code and whether the code should be disclosed, Part III offers two recommendations. First, courts should hold ex parte and in camera proceedings to ascertain the government's interest in nondisclosure. Second, courts should retain their own experts to provide an objective perspective and help judges understand technical information. Applying these procedures will protect both the government's interests and defendants' interests because they will ensure courts have the relevant information to make judicious and informed decisions. Part III reviews the existing framework for evaluating whether sensitive government information should be disclosed in criminal cases, and proposes two procedural changes to augment courts in decisions on the disclosure of NIT code.

A. Existing Balancing Tests Weigh the Government's Interest in Protecting Sensitive Information Against Defendants' Rights and Need to Access the Information

When criminal defendants request access to sensitive government information, courts must first determine whether the information is

material to the defense.[204] If it is material, courts employ a balancing test that weighs the government's interest in nondisclosure against the defendant's need to access the information for their defense. Courts have "broad discretion . . . in deciding whether discovery should be compelled,"[205] but considerations will vary depending on whether the information sought is classified or not. If sensitive information is not classified, but the government has an interest in protecting it, the government will assert a qualified law enforcement privilege. If the information the defendant seeks is classified, procedures under the Classified Information Procedures Act (CIPA) apply.[206] Both contexts are relevant since the FBI has classified the Playpen NIT code and may classify NITs in the future.

The law enforcement privilege that the government has asserted to protect the disclosure of NIT code is rooted in the watershed case, *Roviaro v. United States*.[207] *Roviaro* recognized an "informer's privilege," which allows the government to withhold an informant's identifying information from the defendant to protect "the public interest in effective law enforcement."[208] The Court also established limits on the privilege for fairness purposes: "Where the disclosure of an informer's identity, or of the contents of his communication is relevant and helpful to the defense of an accused, . . . the privilege must give way."[209] The Court did not establish a "fixed rule" and called for "balancing the public interest in protecting the flow of information against the individual's right to prepare his defense."[210] Upon balancing, if a court finds that the information requested is necessary for the defense, but the government insists on nondisclosure, the case must be dismissed.[211] This ensures that the government only withholds information it has a strong interest in concealing and that the defendant's rights are protected.

---

204 *See* United States v. Matish, 193 F. Supp. 3d 585, 598–600 (E.D. Va. 2016) (finding that the defendant failed to prove NIT code was material but "assuming *arguendo*" it had found materiality, "the scales [would] tip substantially in favor of the Government").

205 *In re* Sealed Case, 856 F.2d 268, 271 (D.C. Cir. 1988).

206 *See* 18 U.S.C.A. app. 3 §§ 1–16 (West 2012); *U.S. Attorneys' Manual: Criminal Resource Manual § 2054*, U.S. DEP'T OF JUSTICE, https://www.justice.gov/usam/criminal-resource-manual-2054-synopsis-classified-information-procedures-act-cipa (last visited Aug. 30, 2018) (providing a synopsis of the Classified Information Procedures Act).

207 353 U.S. 53 (1957).

208 *Id.* at 59.

209 *Id.* at 60–61.

210 *Id.* at 62. The balancing test considers factors such as the crime charged, potential defenses, the significance of the informer's testimony, and "other relevant factors." *Id.*

211 *Id.* at 61.

Since *Roviaro*, courts have extended the law enforcement privilege to apply to "sensitive investigative techniques,"[212] recognizing that disclosure can diminish their effectiveness.[213] The inquiry for this law enforcement privilege is one in which "the public interest in nondisclosure must be balanced against the need of a particular litigant for access to the privileged information."[214] The burden rests on the government to demonstrate that the privilege applies.[215] Some factors that courts evaluate include whether the information sought pertains to "law enforcement techniques and procedures,"[216] whether disclosure would interfere with an investigation,[217] whether disclosure "could undermine the safety of law enforcement personnel,"[218] and whether disclosure "would likely undermine 'the ability of a law enforcement agency to conduct future investigations.'"[219]

---

212 United States v. Van Horn, 789 F.2d 1492, 1507–08 (11th Cir. 1986) (holding that a qualified law enforcement privilege applies to the "nature and location of electronic surveillance equipment"); *see also* United States v. Harley, 682 F.2d 1018, 1020–21 (D.C. Cir. 1982) (allowing the government to keep its surveillance location a secret); United States v. Green, 670 F.2d 1148, 1156–57 (D.C. Cir. 1981) (protecting the location of a surveillance post).

213 *See Van Horn*, 789 F.2d at 1508 ("Disclosing the precise locations where surveillance devices are hidden or their precise specifications will educate criminals regarding how to protect themselves against police surveillance. Electronic surveillance is an important tool of law enforcement, and its effectiveness should not be unnecessarily compromised.").

214 *In re* Sealed Case, 856 F.2d 268, 272 (D.C. Cir. 1988) (applying the law enforcement privilege to information related to an SEC investigation). Courts have noted that the balancing analysis differs when considering government disclosures for pre-trial hearings, such as suppression hearings, as opposed to disclosures for trial. *See* United States v. Raddatz, 447 U.S. 667, 679 (1980) (concluding that due process required at a suppression hearing is less demanding than at trial); *see also* United States v. Foster, 986 F.2d 541, 543 (D.C. Cir. 1993) (explaining that a defendant's rights are more limited at a suppression hearing than at trial); United States v. Rigmaiden, 844 F. Supp. 2d 982, 990 (D. Ariz. 2012) (stating the same). In the Playpen cases, defendants have sought disclosure of the full NIT code for trial as well as pre-trial hearings. *See, e.g.*, Darby Motion to Compel, *supra* note 27, at 1 (moving to compel discovery of NIT code for trial and the defendant's motion to suppress). However, since the Playpen NIT has been classified, courts' analysis of the need to disclose the code will differ. *See supra* note 158 and accompanying text; *infra* notes 228–34 and accompanying text.

215 *See In re* City of New York, 607 F.3d 923, 944 (2d Cir. 2010); *see also* United States v. Matish, 193 F. Supp. 3d 585, 597, 601 (E.D. Va. 2016) (finding that the government met its burden in showing the privilege applied).

216 *In re City of New York*, 607 F.3d at 944 (quoting *In re* Dep't of Investigation, 856 F.2d 481, 484 (2d Cir. 1988)).

217 *Id.* (citing *In re Dep't of Investigation*, 856 F.2d at 484).

218 *Id.* at 944–45.

219 *Id.* at 945 (quoting Morrissey v. City of New York, 171 F.R.D. 85, 90 (S.D.N.Y. 1997)); *see also Matish*, 193 F. Supp. 3d at 600–01 (E.D. Va. 2016) (listing examples of law enforcement techniques that courts have found are subject to qualified immunity).

If the government successfully asserts the privilege, it establishes a presumption against disclosure,[220] but the privilege is not absolute.[221] Courts then weigh the defendant's interest in "accurate fact-finding" against the "interests of the public and the police in nondisclosure."[222] If the defendant can make a sufficient showing of need, the government's privilege will give way.[223] Courts can hold a hearing to hear the defendant's claim of necessity,[224] but there are "no fixed rules" in the inquiry and "the necessity determination requires a case–by–case balancing process."[225] Courts consider "the evidence that has already been disclosed to [the] [d]efendant," and whether "there are alternative sources of information upon which [the] [d]efendant can rely."[226] In this way, the balancing framework guards legitimate government interests by "filter[ing] out sensitive evidence that is not genuinely important to the defense," and guarantees that "the defendant cannot be deprived of information so important that the case cannot be tried fairly without it."[227]

CIPA offers more robust procedural safeguards to protect classified information,[228] and was intended to clarify courts' existing powers

---

220 *See In re City of New York*, 607 F.3d at 945 ("[W]e agree with the Seventh Circuit that 'there ought to be a pretty strong presumption against lifting the privilege.'" (quoting Dellwood Farms v. Cargill, Inc., 128 F.3d 1122, 1125 (7th Cir. 1997))).

221 *See id.* at 948 (explaining how this presumption can be rebutted); *see also* United States v. Green, 670 F.2d 1148, 1155–56 (D.C. Cir. 1981) ("The recognition of this privilege, however, cannot be the end of our consideration. . . . [It does] not extinguish a criminal defendant's strong interest in effective cross-examination of adverse witnesses.").

222 *Green*, 670 F.2d at 1156.

223 United States v. Van Horn, 789 F.2d 1492, 1508 (11th Cir. 1986).

224 *See, e.g.*, *id.* ("The district court conducted an in camera hearing to review the government's assertion of privilege and held a hearing on the appellants' claim of necessity.").

225 *Id.*; *see also Green*, 670 F.2d at 1156 (noting that "[c]ourts have employed at least two different methods to balance these competing interests," which include conducting in camera proceedings where the government discloses information to the court or requiring the government to disclose the information to defense counsel under a protective order).

226 United States v. Rigmaiden, 844 F. Supp. 2d 982, 991 (D. Ariz. 2012); *see also* United States v. Cintolo, 818 F.2d 980, 1002 (1st Cir. 1987) (stating that a defendant should show "that there are no adequate alternative means of getting at the same point" (quoting United States v. Harley, 682 F.2d 1018, 1020 (D.C. Cir. 1982))).

227 Serrin Turner & Stephen J. Schulhofer, Brennan Ctr. for Justice, The Secrecy Problem in Terrorism Trials 18 (2005).

228 *Id.* at 18 (describing how CIPA creates more "comprehensive procedures" than *Rovario*). CIPA procedures are designed to "prevent[ ] unnecessary or inadvertent disclosures of classified information." *U.S. Attorneys' Manual: Criminal Resource Manual § 2054*, *supra* note 206 (providing a synopsis of the CIPA). CIPA essentially codified procedures courts were already using in cases involving classified information. Turner & Schulhofer, *supra* note 227, at 19.

to do so under Rule 16.[229] CIPA's goal is to protect classified information and restrict discovery so as not to "impair the defendant's right to a fair trial."[230] Courts have recognized the similarity between a government privilege in classified information and the law enforcement privilege established in *Roviaro*. Thus in analyzing inquiries about the discovery of classified information, courts apply a similar balancing test, considering "whether the material in dispute is discoverable, then whether the material is privileged, but then determin[ing] if the information is at least helpful to the defense."[231]

CIPA allows courts to review information and determine relevancy in closed hearings.[232] However, unlike *Roviaro*, "even if classified information is important to a case, the information still does not necessarily have to be disclosed";[233] CIPA provides three ways for the government to withhold discovery. The government may provide an unclassified and redacted version of the information, an unclassified summary of the information, or a statement admitting the relevant facts that the information would prove.[234] If the court rules that disclosure of classified information is warranted, defense attorneys must receive clearance to access the information.[235] As under *Roviaro*, if the government refuses to disclose classified information where the court orders, the defendant cannot be offered a fair trial, and the indictment must be dismissed.[236]

Under CIPA and Rule 16, courts hold ex parte in camera proceedings to review the government's claims of privilege.[237] Federal

---

229 *See* S. REP. NO. 96-823, at 6 (1980), *as reprinted in* 1980 U.S.C.C.A.N. 4294, 4299 (noting that CIPA § 4 intended to "clarify" courts' "powers under Federal Rule of Criminal Procedure 16(d)(1)").

230 United States v. O'Hara, 301 F.3d 563, 568 (7th Cir. 2002).

231 United States v. Hanna, 661 F.3d 271, 295 (6th Cir. 2011) (quoting United States v. Yunis, 867 F.2d 617, 623 (D.C. Cir. 1989)).

232 TURNER & SCHULHOFER, *supra* note 227, at 19.

233 *Id.* at 20.

234 *Id.* These courts must first approve the use of any of these "substitutions" and should do so only if its use would provide the defendant "'with substantially the same ability to make his defense as would disclosure' of the underlying classified information itself." *Id.* (citing 18 U.S.C.A. app. 3 § 6(c) (2012)).

235 *See* ROBERT TIMOTHY REAGAN, FED. JUDICIAL CTR., KEEPING GOVERNMENT SECRETS: A POCKET GUIDE ON THE STATE-SECRETS PRIVILEGE, THE CLASSIFIED INFORMATION PROCEDURES ACT, AND CLASSIFIED INFORMATION SECURITY OFFICERS 2 (2d ed. 2013) (stating that other than for Article III judges, security clearances are necessary for individuals involved in litigation to view classified documents).

236 *See id.* at 20 ("If the government's secrets cannot be protected adequately while affording the defendant a fair trial, then ordinarily the indictment is dismissed.").

237 *See* United States v. Hanna, 661 F.3d 271, 294–95 (6th Cir. 2011) (holding that the district court did not err in holding an ex parte in camera hearing); United States v. Mejia, 448 F.3d 436, 455–56 (D.C. Cir. 2006) (noting that an ex parte in camera review of the classified information convinced the court that claim to privilege was legitimate); United

Rule of Criminal Procedure 16(d) allows courts to deny, restrict, or defer discovery for "good cause," and permits parties to "show good cause by a written statement" which may be reviewed ex parte.[238] CIPA also allows for ex parte and in camera hearings if the government requests[239] and certifies that one is necessary.[240] Courts generally have broad discretion in holding such proceedings,[241] and among the considerations for doing so is "the protection of information vital to the national security."[242] Ex parte in camera hearings are certainly not required; courts hold them as they see fit.

B. Implementing Procedures to Balance Better

Courts should implement two procedural changes: (1) hold ex parte and in camera proceedings, and (2) employ court experts. Ex parte and in camera proceedings provide forums to ensure courts are apprised of all relevant information about the government's privilege claim and the risks of disclosing sensitive law enforcement information. Where the disclosure of full NIT code is at issue, this Note proposes that courts should always hold ex parte in camera hearings to review the government's position because it allows the government to share sensitive and classified information with courts, such as information pertaining to national security. Otherwise, courts are only informed by the limited information that the government can present in filings responding to the defense and through testimony at hearings with the defense.[243] Recall *Michaud*: The limited information was insufficient for the court to evaluate the government's privilege claim and the stakes of disclosing the full NIT code for the government.[244]

States v. Van Horn, 789 F.2d 1492, 1508 (11th Cir. 1986) (noting that the district court held an in camera hearing to evaluate the government's privilege claim); United States v. Rigmaiden, 844 F. Supp. 2d 982, 991 (D. Ariz. 2012) ("This circuit and other courts have approved *ex parte* hearings for the purpose of considering *Roviaro*-type privilege claims."); United States v. Marzook, 435 F. Supp. 2d 708, 746 (N.D. Ill. 2006) (holding that the lower court's hearing of portions of the suppression hearing ex parte and in camera was consistent with CIPA analysis).

238 FED. R. CRIM. P. 16(d)(1).

239 *See* 18 U.S.C.A. app. 3 § 4 (stating that courts may allow the government to make requests to limit discovery of classified information "to be inspected by the court alone").

240 *See id.* § 6(a).

241 *See Hanna*, 661 F.3d at 294 ("[H]olding such proceedings is within the discretion of the court.").

242 FED. R. CRIM. P. 16 advisory committee's note to 1966 amendment.

243 *See, e.g.*, Michaud Gov't's Response to First Motion to Compel, *supra* note 138, at 15 (noting that disclosure of NIT code "would be harmful to the public interest . . . and possibly lead to other harmful consequences *not suitable for inclusion in this response*") (emphasis added).

244 *See supra* Section II.C.

Ex parte in camera proceedings are valuable to courts' understanding of the government's interest in protecting NIT code—especially the exploit code and vulnerability. They serve as a forum for the government to present sensitive information to the court and allow courts to thoroughly assess the government's interest in nondisclosure. At the same time, courts are able to confirm that the government is not making "frivolous claims of privilege"[245] to unnecessarily withhold information from the defense. The hearings are also an opportunity for courts to determine whether the information requested is relevant to the defense and whether it could be provided by an alternative source. If courts do not hold ex parte in camera hearings, they risk either making decisions that harm the government's interest in protecting sensitive information, if they mistakenly rule disclosure is required, or depriving defendants of their rights, if they mistakenly rule disclosure is not required.

Critics may point out that ex parte proceedings are generally disfavored[246] because they "impair the integrity of the adversary process."[247] The Supreme Court has even stated that a "one-sided determination of facts decisive of rights"[248] can rarely be fair and that "[t]he determination of what may be useful to the defense can properly and effectively be made only by an advocate."[249] However, courts are not limited to making decisions based on the information present at these closed hearings. In addition to an ex parte in camera proceeding to hear the government's claim, courts can also hold a public hearing regarding the defendant's motion to compel discovery.[250] Ex parte in camera hearings are "appropriate if the court has questions about the confidential nature of the information or its relevancy."[251] While such proceedings appear antithetical to an adversarial system, they allow courts to evaluate sensitive information while maintaining

245 United States v. Yunis, 867 F.2d 617, 623 (D.C. Cir. 1989).

246 FED. R. CRIM. P. 16 House Committee on the Judiciary's note to 1975 amendment (stating that "ex parte proceedings are disfavored and not to be encouraged"); United States v. Klimavicius-Viloria, 144 F.3d 1249, 1261 (9th Cir. 1998) ("Ex parte hearings are generally disfavored.").

247 Consol. Response to Gov't's Motion for Reconsiderations; Response to Motions for Ex Parte and In Camera Proceedings; and Second Defense Motion to Dismiss Indictment at 15, United States v. Michaud, No. 3:15-cr-05351-RJB (W.D. Wash. Apr. 25, 2016).

248 United States v. James Daniel Good Real Prop., 510 U.S. 43, 55 (1993) (quoting Joint Anti-Fascist Refugee Comm. v. McGrath, 341 U.S. 123, 170 (1951) (Frankfurter, J., concurring)).

249 Dennis v. United States, 384 U.S. 855, 875 (1966).

250 *See supra* notes 204–05 and accompanying text.

251 *Klimavicius-Viloria*, 144 F.3d at 1261; *see also* FED. R. CRIM. P. 16 House Committee on the Judiciary's note to 1975 amendment ("An ex parte proceeding would seem to be appropriate if any adversary proceeding would defeat the purpose of the protective or modifying order.").

confidentiality. Even when documents and information have been filed under seal and are unavailable to the public, leaks occur,[252] and that is not a risk worth taking with NIT code.

In a similar vein, disclosing NIT code under a protective order also carries risks that the government does not want to take.[253] Given the costs of developing NITs, and the speed at which vulnerabilities can be patched once they are disclosed, any leaks of NIT code disclosed pursuant to a protective order may be devastating for government intelligence operations and ongoing criminal investigations in a matter of hours.[254] Furthermore, it is possible that an individual who acquires access to the code pursuant to a protective order misappropriates it for personal gains by engaging in criminal hacking or selling the code to criminal actors or foreign governments. In these cases, the U.S. government may not know that an individual violated the protective order until the code is used to victimize others or is used against the U.S. Thus, ensuring compliance with a protective order may be difficult,[255] even if it contains robust enforcement provisions. For instance, a protective order that limits review of NIT code to within the confines of a government facility such as an FBI office may not prevent the code from being misappropriated because an expert may memorize parts of the code. As a result, protective orders may not adequately protect public and broader government interests.

Ex parte in camera hearings can shed light on facts that can allow courts to better weigh the government's interests against the defendant's need for information. If the court in *Michaud* had held an ex parte in camera proceeding to allow the government to present information about its concerns regarding disclosure prior to holding the hearing on the defendant's motion to compel discovery, the court may not have reached contradictory conclusions.[256] Furthermore, although these hearings are one-sided and not public, they protect defendants'

---

252 *See, e.g.*, *In re* City of New York, 607 F.3d 923, 937–38 (2d Cir. 2010) (summarizing numerous instances where sensitive information filed under seal was made public).

253 *See, e.g.*, Michaud Gov't's Response to First Motion to Compel, *supra* note 138, at 17 ("Because of the sensitivity of the technique and for other reasons the United States can present at an *ex parte in camera* hearing, disclosing the programming code pursuant to a protective order is inadequate.").

254 *See supra* notes 56–63 and accompanying text.

255 Protective orders typically contain the following provision to address violations of protective orders: "Any violation of any term or condition of this Order by the Defendant [or] any member of the defense team . . . may be held in contempt of court, and/or may be subject to monetary or other sanctions as deemed appropriate by this Court." Discovery Protective Order at 3, *United States v. Michaud*, No. 3:15-cr-05351-RJB (W.D. Wash. Jan. 5, 2016), ECF No. 102; Discovery Protective Order at 2, *United States v. Darby*, No. 2:16-cr-00036-RGD-DEM (E.D. Va. July 6, 2016), ECF No. 44.

256 *See supra* Section II.B.

rights by allowing courts to ensure that the government has a legitimate claim and by preventing unquestioning trust in the government. Consider *United States v. Matish*, where the court declined to hold an ex parte in camera hearing and "place[d] its reliance on the declaration and testimony of [FBI agent] Alfin."[257] While I believe the court reached the right outcome, the court should have held an ex parte in camera hearing. Judges should hold the government accountable and conduct a serious review because the stakes are high for both parties.

In addition to holding ex parte and in camera proceedings, courts should increasingly appoint experts to augment their objective understanding of technical issues in criminal cases where those issues weigh on the merits of parties' claims. This Note proposes a modification in federal courts' use of experts whether they are employed full-time or part-time.[258] Defense and government experts' evaluations inevitably bear biases and frame facts in ways that best serve their party's interests.[259] While this is natural in adversarial proceedings, it can be difficult for courts to separate technical facts from interpretations of those facts. Both parties present information with an angle. Court-appointed experts would serve judges by bolstering their knowledge of important technical information with a more neutral perspective. Where questions about the full NIT code arise, experts would help judges parse out the components of a NIT and understand the technical implications of revealing the exploit code in particular. This knowledge will serve courts well as they try to figure out whether the government is unnecessarily withholding discovery or whether defendants' claims about the potential evidentiary value of the full NIT code are more than "speculative hypotheses."[260]

A structural framework already exists for court-appointed experts and should facilitate courts' wider use of experts. Federal Rule of Evidence 706 states that a "court may appoint any expert that the

---

257 193 F. Supp. 3d 585, 599–600 (E.D. Va. 2016).

258 The costs of courts' increased employment of expert witnesses in criminal cases, separate and apart from experts employed by litigants, are beyond the scope of this Note. However, this would require Congress to appropriate greater funds to the judiciary to finance its use of experts.

259 *Compare* Declaration of Vlad Tsyrklevich, *supra* note 148, at 2–3 (explaining that NITs have four primary components and that the components that the FBI has not produced are necessary for a "complete and accurate analysis"), *with* Declaration of FBI Special Agent Daniel Alfin in Support of Gov't's Motion for Reconsideration at 2, United States v. Michaud, No. 3:15-cr-05351-RJB (W.D. Wash. Mar. 28, 2016), ECF No. 166-2 ("The NIT, however, consists of a single component—that is, the computer instructions delivered to the defendant's computer after he logged into Playpen that sent specific information obtained from his computer back to the FBI.").

260 *Matish*, 193 F. Supp. 3d at 600.

parties agree on and any of its own choosing."[261] The Advisory Committee initially noted that "actual appointment is a relatively infrequent occurrence," but acknowledged that "[t]he inherent power of a trial judge to appoint an expert of his own choosing is virtually unquestioned."[262] Court-appointed experts were also contemplated in Federal Rule of Criminal Procedure 28, but the provision was amended because Rule 706 addressed the matter.[263] Courts should appoint experts they have vetted and with whom they feel comfortable working, since they have the discretion to do so.

To prevent judges who are inclined to favor one party over the other from hiring experts who present a one-sided perspective, court systems can develop lists of vetted experts for judges to choose from. In practice, this may resemble the Foreign Intelligence Surveillance Court's (FISC) recent use of amicus curiae.[264] Even though the scope of the FISC, which considers applications from the government for electronic surveillance on an ex parte basis,[265] is narrower than the federal courts, the court's use of amicus curiae can offer insight on the benefits of court-appointed experts.

The FISC is statutorily required to appoint at least five amicus curiae, which may include individuals "to provide technical expertise, in any instance as [the] court deems appropriate,"[266] and FISC judges may "consider individuals recommended by any source, including members of the Privacy and Civil Liberties Oversight Board."[267] Federal courts may similarly choose to consult Federal Defenders' offices and the Department of Justice. Furthermore, those who serve must have specialized expertise,[268] and be eligible for a security clearance.[269] Such qualifications should also apply to court-appointed experts advising courts on NIT code so they could present at ex parte and in camera hearings to discuss the government's privilege claims.

---

261 FED. R. EVID. 706(a).

262 FED. R. EVID. 706 advisory committee's note to proposed rules.

263 *Id.* ("Subdivision (a) is based on Rule 28 of the Federal Rules of Criminal Procedure, with a few changes, mainly in the interest of clarity."); *see also* FED. R. CRIM. P. 28 advisory committee's note to 1972 amendment (noting that subdivision (a) was "stricken, since the subject of court-appointed expert witnesses is covered in Evidence Rule 706 in detail").

264 *See* USA FREEDOM Act of 2015, Pub. L. No. 114-23, tit. IV, sec. 401, § 103, 129 Stat. 268, 279–80 (to be codified at 50 U.S.C. § 1803(i)) (explaining the procedure for the appointment of amicus curiae in FISC cases).

265 *See* 50 U.S.C. § 1804(a) (2012).

266 USA FREEDOM Act tit. IV, sec. 401, § 103(i)(2)(b).

267 *Id.* § 103(i)(1).

268 *See id.* § 103(i)(3)(a) (requiring individuals to "possess expertise in privacy and civil liberties, intelligence collection, communications technology, or any other area that may lend legal or technical expertise").

269 *Id.* § 103(i)(3)(b).

As law enforcement technology becomes more computer based and technological issues become more prevalent in litigation, court systems should consider hiring full-time experts who may rotate among judges based on need.

By holding ex parte in camera proceedings and working closely with experts, courts will be well equipped to make decisions that hinge on the technical complexities of the technology at issue. With experts, courts will be particularly well poised to consider whether full NIT code or specific lines of code are material to a defendant's case and whether the government should disclose any of it. To be clear, these procedures do not guarantee that courts will reach a certain outcome on the materiality or disclosure of NIT code. I do not suggest that complete NIT code or components of NIT code should never be disclosed. Review should occur on a case–by–case basis, and the government must be as forthcoming as possible without jeopardizing legitimate interests.

Individual review is important for a few reasons. First, it serves to protect the rights of individual defendants. While the FBI was careful in deploying the NIT in the Playpen investigation,[270] and there has been no evidence of impropriety on the Bureau's part, it is not hard to imagine that government operations could go wrong or an agent could try to take advantage of their position.[271] Furthermore, not all NITs are the same. The code of a specific NIT will not need protection forever. Over time, vulnerabilities will be exposed, and some NITs will become obsolete. The government will find ways to exploit different vulnerabilities and continually develop new NITs. Government practices have indicated that the government does not intend to hoard secrets unnecessarily.[272] NIT code has been disclosed in criminal cases,[273] and the decision comes down to whether the NIT remains operative and may be useful in future investigations.

Technological innovations will continue to transform the ways in which law enforcement conduct criminal investigations. More and more law enforcement tools and techniques will rely on sensitive or proprietary code, and leaving courts to make disclosure decisions on case–by–case bases likely will not be efficient or feasible in the long-

---

[270] *See supra* note 124.

[271] *See, e.g.*, Farivar & Mullin, *supra* note 155 (explaining how a DEA agent and a Secret Service agent investigating the Silk Road case were involved in digital currency theft).

[272] The Vulnerabilities Equities Process is intended to ensure that decisions about the disclosure of vulnerabilities are reasoned. *See* FINKLEA, *supra* note 53, at 6–7. And in fact, the government discloses most. Ledgett, *supra* note 132.

[273] *See supra* note 102.

term. The criminal justice system may require broader sweeping legislative action to establish uniform procedures in criminal proceedings. Legislative solutions may begin with modest amendments to CIPA that account for the government's use of malware or may consider innovative ways to curb the use of the trade secret privilege in criminal cases.

Conclusion

NITs are unique. As law enforcement tools that exploit technological vulnerabilities, they play a critical role in investigating cybercrime and in the national security sphere. They identify and locate criminals where traditional investigative techniques fail, and their value lies in their confidentiality. NIT code contains highly coveted exploit code that allows the government to hack into target computers. Disclosing the code can render the NIT useless and jeopardize other government operations. As a result, NITs must be treated much more sensitively than other investigative tools. But the government's interest in confidentiality is inherently in tension with criminal defendants' right to discovery and information material to their defense. The stakes are high for both parties when defendants request to access NIT code.

In order to make informed decisions about materiality and disclosure, courts must be cognizant of the equities at stake and understand some technical details about NITs. They can do so by holding ex parte and in camera proceedings to ascertain the government's interest, and by appointing experts to augment their understanding of technical issues. These procedures will ensure that the government is held accountable, defendants' rights are protected, and NIT code is preserved. As the Dark Web expands, cybercrime becomes more pervasive, and criminal actors devise more sophisticated means of anonymizing their presence online, law enforcement will have to respond creatively to quell threats. In a rapidly changing landscape, there is no permanent solution, and the government's use of tools like NITs will continually evolve. Courts must adapt and be prepared to take on the novel issues that the future holds.