THE COLUMBIA
SCIENCE & TECHNOLOGY
LAW REVIEW

VOL. XIX STLR.ORG FALL 2017

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)[†]

Christine W. Chen[*]

As technology moves toward encryption, law enforcement has turned to creative methods to apprehend criminals attempting to hide or obscure their digital wrongdoings. One such method is the network investigative technique (NIT), which essentially operates by sending a tracking program to users' computer systems to uncover their real IP addresses. Judges can authorize the deployment of NITs through warrants. With the jurisdictional hurdle limiting the reach of such warrants removed by the recent change in Rule 41 of the Federal Rules of Criminal Procedure, the usage of NITs is certain to become more commonplace. However, courts are uncertain about how to treat evidence obtained through NITs, especially with respect to whether defendants are entitled to the full NIT code used against them in the course of discovery. If defendants can access the full code, they could threaten to divulge it to the general public unless prosecutors drop the criminal charges. But if prevented from accessing the code under any circumstances, defendants may be locked into an unfair trial. This Note suggests that courts will need to reformulate the test traditionally used to balance the government's interests and defendants' due process rights with regard to sensitive or confidential information to create a general presumption against releasing the full NIT code.

[†] This Note may be cited as http://stlr.org/cite.cgi?volume=19&article=Chen. This work is made available under the Creative Commons Attribution—Non-Commercial—No Derivative Works 3.0 License.

[*] J.D. Candidate 2018, Columbia Law School. I would like to thank Professor Matthew Waxman for his guidance and the Columbia Science and Technology Review team for their hard work.

I. INTRODUCTION

When some people think of hackers, they envision "somebody sitting on their bed that weighs 400 pounds."[1] In contrast, Federal Bureau of Investigation (FBI) agents do not typically come to mind as stereotypically sophisticated hackers. And yet, it was the FBI who led a large-scale coordinated effort to hack into thousands of

[1] Elizabeth Weise, *Tech Crowd Goes Wild for Trump's '400-Pound Hacker'*, USA TODAY (Sept. 27, 2016, 1:40 PM), http://www.usatoday.com/story/tech/news/2016/09/27/tech-crowd-goes-wild-trumps-400-pound-hacker/91168144/.

computers in connection with a child pornography investigation in 2015.[2] In an operation known as "the Playpen Investigation," the FBI seized a child pornography website's server on the dark web in February 2015 and ran the website for a period of thirteen days in an effort to identify visitors to the website.[3] As visitors' real IP addresses were obscured on the dark web, the FBI deployed what they called "network investigative techniques" (NITs) to website users' computers.[4] The NITs allowed the FBI to unmask users' real identities, leading to at least 137 child pornography-related prosecutions around the United States.[5]

Unsurprisingly, the breadth of the investigation and novelty of NITs have led to inconsistent rulings across the country. Some federal judges have found that the FBI's approach was legal and appropriate.[6] Other judges have found that the FBI's use of NITs

[2] Joseph Cox, *The FBI Hacked Over 8,000 Computers In 120 Countries Based on One Warrant*, VICE (Nov. 22, 2016, 6:18 PM), http://motherboard.vice.com/read/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant.

[3] *Id.*

[4] *Id.*

[5] Joseph Cox, *Dozens of Lawyers Across the US Fight the FBI's Mass Hacking Campaign*, VICE (July 27, 2016, 12:15 PM), https://motherboard.vice.com/read/dozens-of-lawyers-across-the-us-fight-the-fbis-mass-hacking-campaign-playpen.

[6] The majority of district courts where Playpen Investigation cases have been tried found that there was probable cause to issue the NIT warrant. *See, e.g.*, United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263, at *3 n.1 (W.D. Wash. Jan. 28, 2016); United States v. Epich, No. 15-CR-163-PP, 2016 WL 953269, at *1-2 (E.D. Wis. Mar. 14, 2016); United States v. Darby, 190 F. Supp. 3d 520, 532 (E.D. Va. 2016); United States v. Matish, 193 F. Supp. 3d 585, 603-04 (E.D. Va. 2016); United States v. Rivera, No. 15-266, 2016 U.S. Dist. LEXIS 182483, at *25 (E.D. La. July 20, 2016); United States v. Henderson, No. 15-cr-00565-WHO-1, 2016 WL 4549108, at *4 (N.D. Cal. Sept. 1, 2016); United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223, at *7 (W.D. Tex. Sept. 9, 2016); United States v. Jean, 207 F. Supp. 3d 920, 935 (W.D. Ark. 2016); United States v. Knowles, 207 F. Supp. 3d 585, 601 (D.S.C. 2016); United States v. Broy, 209 F. Supp. 3d 1045, 1056-57 (C.D. Ill. 2016); United States v. Anzalone, 208 F. Supp. 3d 358, 367 (D. Mass. 2016); United States v. Smith, No. 4:15-CR-00467, 2016 U.S. Dist. LEXIS 182365, at *21-22 (S.D. Tex. Sept. 28, 2016); United States v. Allain, 213 F. Supp. 3d 236, 244-45 (D. Mass. 2016); United States v. Johnson, No. 15-00340-01-CR-W-GAF, 2016 U.S. Dist. LEXIS 145180, at *18-19 (W.D. Mo. Oct. 20, 2016). Courts have also found that suppression of evidence derived from using the NIT was unwarranted. *See, e.g.*, *Michaud*, 2016 WL 337263, at *6-7; United States v. Stamper, No. 1:15CR109, 2016 WL 695660, at *2-3 (S.D. Ohio Feb. 19, 2016); *Epich*, 2016 WL 953269, at *2; United States v. Werdene, 188 F. Supp. 3d 431, 451-52 (E.D. Pa. 2016); *Darby*, 190 F. Supp. 3d at 533; *Matish*, 193 F. Supp. 3d at 622; *Rivera*, 2016 U.S. Dist. LEXIS 182483, at *16, *20; United States v. Eure, No. 2:16cr43, 2016 WL

in the Playpen Investigation was based on an inappropriately issued warrant and, therefore, suppressed the evidence.[7] Even when finding that the warrant was not properly issued, courts have disagreed on whether the appropriate remedy is to suppress the evidence obtained by the NIT.[8] While much has been discussed regarding the legality of law enforcement usage of NITs,[9] little has been said on the scope of defendants' rights when NITs are used. In particular, are defendants entitled to see the full source code that made them suspects in the first place? Defendants generally have the right to examine the evidence used against them,[10] but this right must be balanced with the possibility of the revealed code falling into the wrong hands. Recognizing the needs of both the defendant and of law enforcement, in one of the cases

4059663, at *9 (E.D. Va. July 28, 2016); United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *7 (C.D. Cal. Aug. 8, 2016); United States v. Adams, No. 6:16-cr-011-Orl-40GJK, 2016 U.S. Dist. LEXIS 105471, at *22-23 (M.D. Fla. Aug. 10, 2016); *Henderson*, 2016 WL 4549108, at *4-6; *Torres*, 2016 WL 4821223, at *7; *Jean*, 207 F. Supp. 3d at 943; *Knowles*, 207 F. Supp. 3d at 600-01; *Broy*, 209 F. Supp. 3d at 1056-59; *Anzalone*, 208 F. Supp. 3d at 370-72; *Smith*, 2016 U.S. Dist. LEXIS 182365, at *11; *Allain*, 213 F. Supp. 3d at 252-53; United States v. Dzwonczyk, No. 4:15CR3134, 2016 U.S. Dist. LEXIS 141297, at *14 (D. Neb. Oct. 5, 2016); United States v. Scarbrough, No. 3:16-CR-035, 2016 WL 5900152, at *1-2 (E.D. Tenn. Oct. 11, 2016); United States v. Libbey-Tipton, No. 1:16 CR 236, 2016 U.S. Dist. LEXIS 182367, at *11-13 (N.D. Ohio Oct. 19, 2016); *Johnson*, 2016 U.S. Dist. LEXIS 145180, at *11-14.

[7] *See* United States v. Levin, 186 F. Supp. 3d 26, 44 (D. Mass. 2016), *vacated*, 874 F.3d 316 (1st Cir. 2017); United States v. Arterbury, No. 15-CR-182-JHP, 2016 U.S. Dist. LEXIS 67092, at *1 (N.D. Okla. May 17, 2016); United States v. Workman, 205 F. Supp. 3d 1256, 1269 (D. Colo. 2016), *rev'd*, 863 F.3d 1313 (10th Cir. 2017); United States v. Croghan (and Horton) (consolidated order), 209 F. Supp. 3d 1080, 1093 (S.D. Iowa 2016), *rev'd*, 863 F.3d 1041 (8th Cir. 2017).

[8] See *supra* note 7, where courts have suppressed evidence. *But see, e.g.*, *Michaud*, 2016 WL 337263, at *8; *Stamper*, 2016 WL 695660, at *3; *Epich*, 2016 WL 953269, at *2; *Werdene*, 188 F. Supp. 3d at 452-53; *Rivera*, 2016 U.S. Dist. LEXIS 182483, at *23-25; *Acevedo-Lemus*, 2016 WL 4208436, at *8; *Adams*, 2016 U.S. Dist. Lexis 105471, at *32; *Torres*, 2016 WL 4821223, at *7; *Henderson*, 2016 WL 4549108, at *6; *Scarbrough*, 2016 WL 5900152, at *2; *Knowles*, 207 F. Supp. 3d at 610; *Broy*, 209 F. Supp. 3d at 1059; *Anzalone*, 208 F. Supp. 3d at 372; *Allain*, 213 F. Supp. 3d at 253; *Libbey-Tipton*, 2016 U.S. Dist. LEXIS 182367, at *19; United States v. Stepus, No. 15-30028-MGM, 2016 WL 6518427, at *2 (D. Mass. Oct. 28, 2016).

[9] *E.g.*, Brian L. Owsley, *Beware of Government Agents Bearing Trojan Horses*, 48 AKRON L. REV. 315 (2015); Steven M. Bellovin et al., *Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet*, 12 NW. J. TECH. & INTELL. PROP. 1 (2014); Susan W. Brenner, *Fourth Amendment Future*, 81 MISS. L.J. 1229 (2012).

[10] FED. R. CRIM. P. 16.

resulting from the Playpen Investigation, Judge Robert J. Bryan of the Western District of Washington came to the contradictory conclusion that the federal government is entitled to withhold full access to the NIT code but also that the information should be handed over to the defense.[11]

This Note argues that courts should apply a heightened standard of relevance, resulting in the general presumption that NIT code is not discoverable, while still balancing the risks of divulging the entire NIT source code with the code's probative value. Part II describes what NITs are, explains why law enforcement uses them, and details arguments for and against letting defendants have access to the entire NIT code used to reveal their IP addresses. Part III considers the current approach courts take when sensitive information is at stake and how involvement of classified information or foreign intelligence can complicate that approach. Part IV takes the experiences and lessons from this approach to create an alternative doctrinal approach for courts to encourage judicial economy, wherein defendants are not entitled to NIT code barring a few narrow exceptions. NITs will become powerful and necessary investigative tools in the near future, so courts must craft a coherent policy toward NIT-related discovery sooner rather than later.

II. BACKGROUND

The change to Rule 41 of the Federal Rules of Criminal Procedure, operational as of December 1, 2016,[12] effectively

[11] Order on Procedural History and Case Status in Advance of May 25, 2016 Hearing at 5, *Michaud*, 2016 WL 337263 (No. 3:15-cr-05351-RJB), ECF No. 205 ("The resolution of Defendant's Third Motion to Compel Discovery places this matter in an unusual position: the defendant has the right to review the full N.I.T. code, but the government does not have to produce it. Thus, we reach the question of sanctions: What should be done about it when, under these facts, the defense has a justifiable need for information in the hands of the government, but the government has a justifiable right not to turn the information over to the defense?").

[12] FED. R. CRIM. P. 41(b)(6). The current rule modifies the old rule by adding the following: "(6) a magistrate judge with authority in any district where activities related to a crime may have occurred has authority to issue a warrant to use remote access to search electronic storage media and to seize or copy electronically stored information located within or outside that district if:

(A) the district where the media or information is located has been concealed through technological means; or

(B) in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts."

cemented federal law enforcement's usage of NITs. Under the new Rule 41, magistrate judges can issue warrants in instances where geographical jurisdiction is unclear, such as where a suspect has hidden the location of his computer or where the crime being investigated involves widespread hacking of victim computers.[13] This obviates many of the territorial arguments that had been made against NITs. For example, defense counsel could argue under the old Rule 41 that a magistrate judge in one state did not have the authority to issue an NIT warrant that would invade hundreds or thousands of computers located in many other states. Under the new Rule 41, magistrate judges are explicitly allowed to issue warrants to obtain electronically stored information outside of their judicial district. In situations where the location of the information sought may be unknown because of the defendant's concealment efforts, the new Rule 41 gets rid of any territorial limitations in the way of such an investigation.

Consequently, it seems probable that the government will conduct more investigations that rely upon NITs, leading to more prosecutions reliant on evidence gained from them in many different jurisdictions. Courts, however, have very little guidance on how to proceed in NIT-related cases. NITs bring features normally associated with the intelligence community like the regular use of classified information into the domain of domestic criminal law. For example, some of the Playpen Investigation defendants have asked courts to compel law enforcement to turn over the full NIT codes used to access defendants' computers.[14] Prosecutors have been willing to turn over some parts of the code, but have been steadfast in refusing to give the defense the "exploit," which is the code used to enter the defendant's device.[15] Since the usage of NITs is only recently becoming more prevalent, courts must craft an approach using principles from various other fields of law that is fair to both defendants and prosecutors.

[13] Leslie R. Caldwell, *Rule 41 Changes Ensure a Judge May Consider Warrants for Certain Remote Searches*, DOJ (June 20, 2016), https://www.justice.gov/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches.

[14] Cyrus Farivar, *Feds May Let Playpen Child Porn Suspect Go to Keep Concealing Their Source Code*, ARS TECHNICA (Jan. 9, 2017, 4:39 PM), https://arstechnica.com/tech-policy/2017/01/feds-may-let-playpen-child-porn-suspect-go-to-keep-concealing-their-source-code/.

[15] Memorandum in Opposition to Defendant's Motions to Compel and to Dismiss at 9, United States v. Palaniappan, No. 15-cr-485 (E.D.N.Y. filed Sept. 1, 2015), ECF No. 33.

A. What Are NITs?

As innocuous and bland as "network investigative techniques" sounds, NITs actually describe malicious software, or malware, used by law enforcement to hack targets' computer systems.[16] While the specifics and targets of the malware used can differ, NITs generally consist of four components: (1) a generator, (2) an exploit, (3) a payload, and (4) a logging server.[17]

The generator establishes a unique ID for the website visitor and transmits the exploit, ID, and payload to the visitor's computer.[18] The exploit is the component that creates access for the payload to enter the target computer.[19] The payload is the executing program, and for NITs, the goal is usually to search and collect information.[20] When considering the different types of payloads that exist, NITs are closer to cyberexploitation than to cyberattacks in that the goal of the intrusion is not to disrupt the target, but rather to exploit the information available or to passively observe a network's activity.[21] Finally, the logging server runs on law enforcement servers and receives and records the information seized by the payload.[22]

To transmit the payload, law enforcement must first enter the target system using vulnerabilities.[23] They can do so via at least two different paths: (1) "spear phishing," where specific individuals are targeted or (2) "watering hole" operations, where any and all visitors to a network are targeted.[24] In spear phishing, investigators

[16] 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/.

[17] 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.

[18] *Id.*

[19] *Id.*

[20] *Id.*; Bellovin et al., *supra* note 9, at 25.

[21] TECHNOLOGY, POLICY, LAW, AND ETHICS REGARDING U.S. ACQUISITION AND USE OF CYBERATTACK CAPABILITIES 80-81, 170 (William A. Owens et al. eds., 2009).

[22] Hennessey & Weaver, *supra* note 17.

[23] Bellovin et al., *supra* note 9, at 24.

[24] Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1097 (2017); Jonathan Mayer, *Constitutional Malware* 13-14 (Sept. 14, 2016) (draft paper), https://ssrn.com/abstract=2633247. Other methods include man-in-the-middle attacks where "an active attacker interrupts the connection between the target and another resource and surreptitiously inserts itself as an intermediary."

send a communication, like an e-mail or a social media message, to the target in an effort to get the target to unknowingly download the malware.[25] For a watering hole delivery, as was used in the Playpen Investigation, law enforcement takes over an operating server and uses it to distribute the malware.[26]

Once installed on the target device or devices, the payload is executed and can compel the target to take various actions like establishing a remote connection and executing a series of commands.[27] For example, in a 2011 child pornography investigation called Operation Torpedo, the FBI used a NIT through a Flash application that would identify a user's real IP address, bypassing measures in the Tor network that protect user identity.[28] Once that information was sent back to law enforcement, they were able to unmask the previously anonymous users through their real IP addresses. As was the process in the Playpen Investigation, law enforcement agents can then seek another warrant for the district in which each of the targeted

Bellovin et al., *supra* note 9, at 20. Mayer notes other methods like physical installations or enlisting a third party to help. Mayer, *supra*. While unconfirmed, it is possible that the FBI has also taken advantage of zero-day vulnerabilities, which are vulnerabilities that are unknown to the software developer. Ahmed Ghappour, *Is the FBI Using Zero-Days in Criminal Investigations?*, JUST SECURITY (Nov. 17, 2015), https://www.justsecurity.org/27705/law-enforcement-zero-days/.

[25] Mayer, *supra* note 24, at 13 n.35.

[26] Zach Lerner, Note, *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, 40-42 (2016) (describing the phishing and watering hole strategies). An expert witness for the defense described the NIT procedure in this way: "The NIT presented by the FBI works by using an 'exploit,' a piece of software that takes advantage of a software 'vulnerability' in the Tor Browser program. By exploiting this software vulnerability, the NIT is able to circumvent the security protections in the Tor Browser, which under normal circumstances, prevents web sites from determining the true IP address or MAC address of visitors. After exploiting the vulnerability, the NIT delivers a software 'payload,' a predetermined set of actions, to computers that receive the payload (the 'host computer'). The payload used by the FBI in this case collected and then transmitted identifying information about the host computer (including its IP address) along with a unique 'identifier' used to associate the target with the identifying information that the NIT collects." Declaration of Vlad Tsyrklevich at 2, United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263 (W.D. Wash. Jan. 14, 2016), ECF No. 115-1.

[27] Bellovin et al., *supra* note 9, at 26.

[28] Joseph Cox, *The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers*, VICE (Jan. 5, 2016, 4:00 PM), http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers.

devices' real IP addresses is located, search the devices themselves, and gather evidence of the alleged crime.[29]

B. Why Is Law Enforcement Using NITs?

Technological advancement is a wonderful thing. Almost two-thirds of Americans own smartphones,[30] eighty-four percent of adult Americans have access to the Internet,[31] and companies have increasingly found ways to insert technology into everyday lives.[32] But the rapid advancement in consumer technology comes hand-in-hand with advancements in software that consumers can use to cover their digital tracks. These developments have strained law enforcement's ability to "intercept and access communications and information pursuant to court orders,"[33] a phenomenon termed "Going Dark."[34] Encryption, in particular, has prevented law enforcement from gathering information from communications providers, even when presented with court-issued warrants.[35]

Encryption, which protects data and communications from unauthorized persons, is now commonly used to protect messages or Internet search histories.[36] Because so much is now digitalized, encryption is crucial to protecting against cyberattacks and

[29] Orin Kerr, *Government 'Hacking' and the Playpen Search Warrant*, WASH. POST (Sept. 27, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/09/27/government-hacking-and-the-playpen-search-warrant/.

[30] Aaron Smith, *U.S. Smartphone Use in 2015*, PEW RES. CTR. (Apr. 1, 2015), http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.

[31] Andrew Perrin & Maeve Duggan, *Americans' Internet Access: 2000-2015*, PEW RES. CTR. (June 26, 2015), http://www.pewinternet.org/2015/06/26/americans-internet-access-2000-2015/.

[32] This is demonstrated by the prevalence of the "Internet of Things," where any and all things, like washing machines, are being connected to the Internet. Jacob Morgan, *A Simple Explanation of 'The Internet of Things'*, FORBES (May 13, 2014, 12:05 AM), http://www.forbes.com/sites/jacobmorgan/2014/05/13/simple-explanation-internet-things-that-anyone-can-understand/#261e2a7c6828.

[33] *Going Dark*, FBI, https://www.fbi.gov/services/operational-technology/going-dark (last visited Feb. 8, 2017).

[34] *Id.*; HOUSE HOMELAND SEC. COMM., GOING DARK, GOING FORWARD: A PRIMER ON THE ENCRYPTION DEBATE (2016), https://homeland.house.gov/wp-content/uploads/2016/07/Staff-Report-Going-Dark-Going-Forward.pdf.

[35] *Going Dark*, *supra* note 33.

[36] *What is Encryption?*, ELEC. FRONTIER FOUND., https://ssd.eff.org/en/module/what-encryption (last visited Feb. 8, 2017).

invasions of privacy.[37] One estimate says that businesses lose as much as $400 billion per year due to cybercrime.[38]

While encryption closes the door to potential hacking, it also closes the door to law enforcement investigations.[39] In September 2014, Apple stirred much debate on this issue when it announced that its iPhones would have single key encryption, meaning that Apple would be unable to unlock iPhones run on its latest operating system, even if presented with a warrant.[40]

Security experts have strongly recommended against creating backdoors for government agencies, arguing that these configurations make systems more vulnerable to hackers and create precedent for authoritarian foreign governments to demand similar levels of access.[41] Backdoors are often unknown to users but generally allow administrators remote access to the software or computer system, often for maintenance purposes.[42] Backdoors can also give government agencies remote access for intelligence or law enforcement purposes as well.[43]

Companies certainly seem to agree with security experts against the wisdom of backdoors; following in the steps of Apple's announcement, Facebook[44] and WhatsApp[45] implemented end-to-end encryption for their billions of users. End-to-end encryption

[37] Ellen Nakashima & Barton Gellman, *As Encryption Spreads, U.S. Grapples with Clash Between Privacy, Security*, WASH. POST (Apr. 10, 2015), https://www.washingtonpost.com/world/national-security/as-encryption-spreads-us-worries-about-access-to-data-for-investigations/2015/04/10/7c1c7518-d401-11e4-a62f-ee745911a4ff_story.html.

[38] Steve Morgan, *Cyber Crime Costs Projected to Reach $2 Trillion by 2019*, FORBES (Jan. 17, 2016, 11:01 AM), http://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#1dc34a483bb0.

[39] HOUSE HOMELAND SEC. COMM., *supra* note 34.

[40] Nakashima & Gellman, *supra* note 37.

[41] Salvador Rodriguez, *Cybersecurity Experts Recommend Against Encryption Backdoors for Government Agencies*, INT'L BUS. TIMES (July 7, 2015, 8:09 PM), http://www.ibtimes.com/cybersecurity-experts-recommend-against-encryption-backdoors-government-agencies-1998670.

[42] Kim Zetter, *Hacker Lexicon: What Is a Backdoor?*, WIRED (Dec. 11, 2014, 6:35 AM), https://www.wired.com/2014/12/hacker-lexicon-backdoor/.

[43] *Id.*

[44] Kate Conger, *Facebook Messenger Adds End-to-End Encryption in a Bid to Become Your Primary Messaging App*, TECHCRUNCH (July 8, 2016), https://techcrunch.com/2016/07/08/messenger-adds-end-to-end-encryption/.

[45] Cade Metz, *Forget Apple vs. the FBI: WhatsApp Just Switched on Encryption for a Billion People*, WIRED (Apr. 5, 2016, 11:00 AM), https://www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/.

means that only the sender and recipient of a message have the "keys" needed to decipher the message, and third parties would not be able to understand the communication if they intercepted it.[46]

Instead of encouraging system weaknesses through backdoors and dissuading the movement towards encryption, law enforcement can turn to NITs to take advantage of holes already present in the system. Indeed, the Obama administration appeared to have embraced this strategy in the intelligence and defense arenas when it breathed new life into the White House vulnerability equities process (VEP).[47] The VEP is "an internal framework for determining when and whether the US government should publicly disclose newly-discovered software and hardware vulnerabilities—both those independently discovered by federal agencies or in some cases acquired from third-party contractors."[48] While the exact nature of the VEP is classified, the process generally works by balancing the public's "need to know" against the benefits of keeping such vulnerabilities secret for operational use.[49]

The spread of encryption will necessitate that law enforcement turn to hacking as an investigative tool in the future. Backdoors are increasingly no longer a viable option for agents to obtain access to devices, with or without a warrant. Consequently, tools like NITs will allow law enforcement to bypass encryption and features that anonymize users in an attempt to stave off the Going Dark phenomenon.

C. NIT Evidence in the Context of Defendants' Rights

While the methods to obtain evidence have changed, the underlying concerns of providing defendants with a fair trial have not. Defendants in NIT-related cases, like in any other criminal cases, are entitled to discovery and the fundamental right to due process.

[46] Lee Bell, *Encryption Explained: How Apps and Sites Keep Your Private Data Safe (and Why That's Important)*, WIRED (June 5, 2017), http://www.wired.co.uk/article/wired-explains-encryption-how-do-apps-keep-our-private-data-safe.

[47] Dave Aitel & Matt Tait, *Everything You Know About the Vulnerability Equities Process Is Wrong*, LAWFARE (Aug. 18, 2016, 2:46 PM), https://www.lawfareblog.com/everything-you-know-about-vulnerability-equities-process-wrong.

[48] *Id.*

[49] *Id.*

Arguments for access to the full NIT code have primarily been grounded in Rule 16(a)(1)(E) of the Federal Rules of Criminal Procedure.[50] The Rule says that "[u]pon a defendant's request, the government must permit the defendant to inspect and to copy or photograph books, papers, documents, data, photographs, tangible objects, buildings or places, or copies or portions of any of these items if the item is within the government's possession, custody, or control and: (i) the item is material to preparing the defense; (ii) the government intends to use the item in its case-in-chief at trial; or (iii) the item was obtained from or belongs to the defendant."[51] Consequently, defendants may argue they need the full code in order to prepare for their defense.

However, what can be considered material to preparing the defense? Materiality is a broad standard that encompasses anything that can be used to counter the government's case or to support the defense's arguments.[52] It certainly includes discovery of exculpatory evidence.[53] Even inculpatory evidence may be material since a "defendant who knows that the government has evidence that renders his planned defense useless can alter his trial strategy."[54] Without the complete right to present a defense, a trial becomes merely a platform for the prosecution to present uncontested evidence.[55]

Most importantly, defendants may need evidence in the government's hands to make adequate constitutional trial rights arguments. The Constitution, mainly in the Fifth and Sixth Amendments, guarantees defendants basic rights in order to ensure that criminal proceedings are fair and transparent.[56] These rights include the right to confront the evidence and witnesses, the right to a public trial, the right to a jury trial, and the requirement that guilt be proven beyond a reasonable doubt.[57] Due process

[50] *See, e.g.*, United States v. Palaniappan, No. 15-cr-485 (E.D.N.Y. filed Sept. 1, 2015).

[51] FED. R. CRIM. P. 16(a)(1)(E).

[52] United States v. Stevens, 885 F.2d 1175, 1180 (2d Cir. 1993).

[53] *See* United States v. Bagley, 473 U.S. 667 (1985).

[54] United States v. Muniz-Jaquez, 718 F.3d 1180, 1183 (9th Cir. 2013).

[55] Thomas G. Stacy, *The Constitution in Conflict: Espionage Prosecutions, the Right to Present a Defense, and the State Secrets Privilege*, 58 U. COLO. L. REV. 177, 198 (1988).

[56] SERRIN TURNER & STEPHEN J. SCHULHOFER, THE SECRECY PROBLEMS IN TERRORISM TRIALS 10-11 (2005).

[57] *See* U.S. CONST. amends. V & VI. The right of the defendant to obtain exculpatory evidence in the government's possession is not explicitly found in the Constitution, but the Supreme Court has held the right to be implicit in the Constitution's guarantee of due process. Brady v. Maryland, 373 U.S. 83 (1963).

also ensures that defendants are entitled to evidence in their favor that is material to findings of prosecutorial missteps.[58]

The full NIT code may be needed to show that the government violated the defendant's due process rights. The code could potentially show that law enforcement exceeded the scope of the search warrant,[59] that a third party or even government placed the incriminating evidence to frame the defendant,[60] or that the government misled the courts in its presentation of the case.[61] These are legitimate factors to consider when deciding whether defendants are entitled to access the entirety of the NIT source code used to find them.

The Confrontation Clause of the Sixth Amendment is particularly relevant to the issue of the disclosure of the NIT code. The Confrontation Clause is key to the adversarial process in that it mandates that the prosecution cannot hide evidence that it plans to use from the defendant and also ensures that the defendant is present to respond to the evidence against him.[62] Although counsel may be present at proceedings without the defendant, removing the defendant from even small parts of the discovery process potentially impedes counsel's ability to make effective arguments, since defendants are often the most important source of information for the defense.[63]

D. The Danger of Giving Defendants Access to Complete NIT Source Code

The government is steadfastly sticking to the position that they will not reveal the entire NIT source code, claiming law enforcement privilege. Government prosecutors have been willing to turn over parts of the code, but they resolutely take the position that the exploit should not be disclosed.[64] Disclosing the exploit could harm the public interest as "[d]isclosure of this information

[58] *Brady*, 373 U.S. at 87. A materiality showing under *Brady* requires a reasonable probability that the result would be different if the government had disclosed the evidence sought. United States v. Caro, 597 F.3d 608, 619 (4th Cir. 2010).

[59] Motion to Compel at 10, United States v. Palaniappan, No. 15-cr-485 (E.D.N.Y. filed Sept. 1, 2015), ECF No. 28.

[60] *Id.*

[61] State v. Andrews, 134 A.3d 324 (Md. Ct. Spec. App. 2016).

[62] TURNER & SCHULHOFER, *supra* note 56, at 12.

[63] *Id.*

[64] Stephanie Lacambra, *Why the Government Must Disclose Its Exploit to the Defense in the Playpen Cases*, ELEC. FRONTIER FOUND. (Nov. 2, 2016), https://www.eff.org/deeplinks/2016/10/why-government-must-disclose-its-exploit-defense-playpen-cases.

could diminish the future value of significant investigative techniques, allow individuals to devise measures to counteract these techniques in order to evade detection, and discourage cooperation from third parties and other governmental agencies who rely on these techniques in critical situations."[65]

Turning over the exploit code has two negative effects on law enforcement efforts. First, it identifies the existing vulnerability, which could diminish future efforts to identify other suspects in similar investigations, child pornography cases, or otherwise.[66] Once the vulnerability is exposed, it can be fixed, and thus an NIT code, used to great success in the past, may become useless. Second, the actual lines of code are "implicated in highly sensitive law enforcement, military, and intelligence activity."[67] Compromising here with the defense could threaten a range of vital national interests. If a criminal defendant leaks a crucial part of the code, his actions negatively affect not only other criminal investigations related to the same NIT used against him, but potentially also military or intelligence projects exploiting the same or similar vulnerabilities as well.

Without the relevant safeguards in place, a leaked NIT source code could become a national security issue. Although the government avoids using the word "hack," NITs are at their heart a means of accessing computers without the user's consent. Releasing the code could mean enabling criminal hackers. In particular, turning over the code to the defendant could lead to a version of "graymailing," which refers to the practice of defendants threatening to disclose classified information as part of their defense.[68] It is not difficult to imagine that an immoral defendant would threaten to leak the code to the public if charges were not

[65] Response to Motion to Compel at 10, United States v. Palaniappan, No. 15-cr-485 (E.D.N.Y. filed Sept. 1, 2015), ECF No. 33; *see also* United States v. Rigmaiden, 844 F. Supp. 2d 982, 994 (D. Ariz. 2012) ("Disclosure would enable adversaries of law enforcement to defeat electronic surveillance operations and to avoid detection by such surveillance. Disclosure of the information would also place law enforcement agents at risk when conducting such surveillance. Disclosures of the specific identities of agents involved in this operation could jeopardize their safety and would effectively eliminate them as law enforcement assets used in electronic surveillance. With only a limited number of individuals trained and skilled in operating this equipment, disclosure would therefore seriously hamper law enforcement efforts.").

[66] Hennessey & Weaver, *supra* note 17.

[67] *Id.*

[68] RICHARD ZABEL & JAMES J. BENJAMIN, JR., HUMAN RIGHTS FIRST, IN PURSUIT OF JUSTICE: PROSECUTING TERRORISM CASES IN THE FEDERAL COURTS 82 (2008).

dropped. Without the NIT code under strict government control, third-party companies and institutions become more vulnerable to hacking by malicious third parties who have taken advantage of a sensitive law enforcement tool. If the government prevents access to the NIT code, the defendant never gains this leverage in the first place.

A central feature of classified or sensitive information is that it is on a "need to know" basis.[69] If the defense can adequately put forth a strong argument without the need for access to sensitive materials, this information remains and should remain under the protection of the government.[70]

E. Short Overview of NIT-Related Discovery Decisions

The issue of whether to turn over full NIT codes to defendants has been litigated in a few lower courts with varying outcomes. In *United States v. Michaud*, the judge ruled that the entire code had to be turned over;[71] this was perhaps the reason why the government declined to pursue the prosecution in the end.[72] Both *United States v. Darby* and *United States v. Matish*, among others also arising out of the Playpen Investigation, rejected the defendant's motion to compel disclosure.[73] It is clear that, despite originating from the same NIT code, courts disagree on this issue, and this is leading to unjustifiably disparate outcomes.

Before the Playpen cases, a defendant in a similar investigation—also involving child pornography and an anonymizing web browser—also sought the original source code for the NIT used against him.[74] Here, the FBI did not develop the code and instead took the source from a public website.[75] The

[69] Melanie Reid, *Secrets Behind Secrets: Disclosure of Classified Information Before and During Trial and Why CIPA Should Be Revamped*, 35 SETON HALL LEGIS. J. 272, 293 (2011).

[70] *Id.*

[71] Order on Procedural History and Case Status in Advance of May 25, 2016 Hearing, United States v. Michaud, No. 3:15-cr-05351-RJB, 2016 WL 337263 (W.D. Wash. May 18, 2016), ECF No. 205.

[72] Order Dismissing Indictment Without Prejudice, *Michaud*, 2016 WL 337263 (No. 3:15-cr-05351-RJB), ECF No. 225.

[73] United States v. Darby, No. 2:16cr36, 2016 WL 3189703 (E.D. Va. June 3, 2016); United States v. Matish, No. 4:16cr16, 2016 WL 3545776 (E.D. Va. June 23, 2016).

[74] United States v. Cottom, Nos. 8:13CR108; 8:15CR239, 2015 U.S. Dist. LEXIS 171880 (D. Neb. Dec. 22, 2015), *aff'd*, No. 16-1050, 2017 U.S. App. LEXIS 2789 (8th Cir. Feb. 17, 2017).

[75] *Id.* at *6-8.

government could not produce the source code as it was improperly preserved, but the court, in denying the related motion to suppress, relied heavily upon the defendant's own expert witnesses' statements that the "availability of the source code would not affect their conclusions."[76] It is unclear whether the court would have ordered the government to turn over the full code had it still existed when the defendant had requested it, as the government did not argue that the defendant was not entitled to the full source code.

III. THE CURRENT APPROACH

Given that courts disagree over whether to compel prosecutors to disclose the entire NIT code, it is clear that a new, more well-defined approach to this problem is needed. Neither extreme, of either continually obligating prosecutors to turn over the code or of steadfastly blocking defendants from accessing the entire code, is adequate to deal with the sensitivities in these sorts of law enforcement hacking cases. As hinted above, the former increases the chances of a disastrous leak impacting other areas of national interest, and the latter encourages unchecked governmental overreach. After determining materiality, courts have thus far used the *Roviaro* balancing test (described below) to determine whether defendants' rights trump law enforcement privilege but have arrived at varying outcomes.[77] In addition, in some instances, the resource-draining measures[78] outlined in the Classified Information Procedures Act (CIPA) may apply if law enforcement has moved to keep the NIT code secret.[79]

A. Finding Materiality

Defendants must first overcome the Rule 16 requirement for materiality in the Federal Rules of Criminal Procedure. As mentioned above, it is a low standard in that information need only be "helpful to the defense" to be considered material.[80] However, a defendant cannot merely claim that evidence is material, but "must 'show' 'more than that the [item] bears some

[76] *Id.* at *22-23.

[77] Roviaro v. United States, 353 U.S. 53 (1957).

[78] TURNER & SCHULHOFER, *supra* note 56, at 25.

[79] Andrew Dalton, *FBI Moves to Keep Its Tor Hacking Tool Secret*, ENGADGET (June 24, 2016), https://www.engadget.com/2016/06/24/fbi-moves-to-keep-its-tor-hacking-tool-secret/.

[80] United States v. Vue, 13 F.3d 1206, 1208 (8th Cir. 1994).

abstract logical relationship to the issues in the case.'"[81] Once materiality is established, the court can then engage in the *Roviaro* balancing test.

B. Roviaro v. United States

Roviaro is the seminal case on the battle between law enforcement privilege and defendants' rights. It established a qualified informant privilege, which has been expanded over the years to encapsulate a general law enforcement privilege. This is a higher threshold than the one set by the materiality requirement. For example, inculpatory evidence would be material to a criminal defendant's case, but it may not be relevant and helpful, as *Roviaro* requires.

Albert Roviaro was indicted in 1955 for selling heroin in Chicago.[82] The indictment alleged that he had sold to a "John Doe," and while he moved to uncover John Doe's identity, the district judge denied his motion.[83] Doe never testified, but the prosecution did rely on the testimony of federal and local law enforcement officers who worked with Doe.[84] One of the officers hid in the trunk of Doe's car and heard the conversation between Roviaro and Doe, witnessing the drug sale.[85]

The Supreme Court found that, like other evidentiary privileges, the informant's privilege inhibits fair fact-finding but is needed for policy reasons.[86] The informant's privilege is needed for effective law enforcement; preserving the anonymity of informers encourages people to help law enforcement.[87] However, unlike many other evidentiary privileges, this type of privilege is limited. One of the limitations is fairness—"[w]here the disclosure of an informer's identity, or of the contents of his communication, is *relevant and helpful* to the defense of an accused, or is essential to a fair determination of a cause, the privilege must give way."[88] To

[81] United States v. Jordan, 316 F.3d 1215, 1250-51 (11th Cir. 2003) (citing United States v. Buckley, 586 F.2d 498, 506 (5th Cir. 1978)).

[82] *Roviaro*, 353 U.S. at 55.

[83] *Id.*

[84] *Id.* at 56-57.

[85] *Id.* at 57.

[86] Matthew D. LaBrie, *The Common Interest Privilege*, ABA (Sept. 30, 2014), https://apps.americanbar.org/litigation/committees/trialevidence/articles/fall2014-0914-common-interest-privilege.html.

[87] *Roviaro*, 353 U.S. at 59.

[88] *Id.* at 60-61 (emphasis added). The circuit courts are actually unclear about whether *Roviaro* stands for privilege always giving way when material is

balance these interests, a court would need to consider "the crime charged, the possible defenses, the possible significance of the informer's testimony, and other relevant factors."[89] Under this formulation, the government is able to withhold evidence that is both not relevant and helpful, but it is forced to turn over evidence when it is relevant and helpful. If the government still does not want to turn over relevant and helpful evidence after the court determines the *Roviaro* test favors the defendant, its only option would be to drop the criminal charges.[90] Disclosure is not a real possibility for the government if it fought vigorously against disclosure. So, in reality, the government would be forced to drop the charges.

Cases like *United States v. Van Horn* expanded the informant's privilege to other areas of law enforcement. In *Van Horn*, defendants in a marijuana drug ring under electronic surveillance made demands in discovery for the type of microphone used and the location of where the microphone was hidden.[91] They argued that being denied this information amounted to being deprived of the right to confrontation, while the government maintained that revealing the information would negatively impact future criminal investigations.[92] Ruling that the defendants had not shown the requisite necessity of this evidence for their case, the court also stressed that "determination requires a case by case balancing process, and that [it had] established no fixed rules about the discoverability of electronic surveillance techniques in criminal cases."[93]

The balancing test must also take into account the reason why disclosure is needed at a particular stage of a criminal case. Applying *McCray v. Illinois*, the court in *United States v. Rigmaiden* considered that the defendant sought discovery for a

relevant and helpful, United States v. Moussaoui, 382 F.3d 453, 476 (4th Cir. 2004), or when the information would be relevant and helpful, a court conducts the balancing test between the public interest and the defendant's need for the information, United States v. Klimavicius-Viloria, 144 F.3d 1249, 1261 (9th Cir. 1998). Other circuits also hold that balancing is appropriate in CIPA cases. *See* United States v. El-Mezain, 664 F.3d 467, 523 (5th Cir. 2011); United States v. Smith, 780 F.2d 1102, 1106 (4th Cir. 1985) (en banc).

[89] *Roviaro*, 353 U.S. at 62.

[90] THOMAS J. GARDNER & TERRY M. ANDERSON, CRIMINAL EVIDENCE: PRINCIPLES AND CASES 166 (2013).

[91] United States v. Van Horn, 789 F.2d 1492, 1507 (11th Cir. 1986).

[92] *Id.*

[93] *Id.* at 1508.

motion to suppress, not for trial.[94] The evidentiary requirements for a suppression hearing are lower than that for trial. For example, issuance of a search warrant requires only probable cause, whereas conviction requires evidence beyond a reasonable doubt.[95] In other words, the government is permitted to meet a lower standard for withholding sensitive information during discovery.

These cases illustrate that law enforcement privilege is qualified by the defendant's need for information. As compared to demonstrating materiality, the defendant must make a heightened showing of necessity and cannot rely on purely hypothetical ways that the evidence would be "tangible" or "helpful." The cases also demonstrate the flexible and ambiguous nature of the balancing test, taking into account factors such as the potential application of the evidence in controversy.

C. Applying the Classified Information Procedures Act (CIPA)

Cases after *Roviaro* also established the practice of *ex parte* hearings in order to review the sensitive information that is at the basis of the government's privilege claims.[96] The Classified Information Procedures Act (CIPA) codifies the procedure for when the evidence is classified. Under CIPA, the government does not have to choose between bringing charges against a defendant and protecting classified information.[97] While CIPA governs the usage of classified evidence by both the prosecution and the defense, this discussion will only focus on when a defendant seeks the disclosure of classified information from the prosecution.

The government must invoke CIPA by first motioning for a protective order "against the disclosure of any classified information disclosed by the United States to any defendant in any criminal case."[98] The motion for the protective order provides background information such as an "overview on national security

[94] United States v. Rigmaiden, 844 F. Supp. 2d 982, 989-90 (D. Ariz. 2012) (citing McCray v. Illinois, 386 U.S. 300 (1967)).

[95] *Id.* at 990 (quoting *McCray*, 386 U.S. at 311) (reading *Roviaro* to hold that, even at trial, there is no "absolute rule requiring disclosure of an informer's identity," much less "where the issue is the preliminary one of probable cause, and guilt or innocence is not at stake").

[96] *See, e.g.*, United States v. Johns, 948 F.2d 599, 606 (9th Cir. 1991) (approving district court's *ex parte* hearing to evaluate the government's request to protect the informant's identity despite defendant's objections).

[97] TURNER & SCHULHOFER, *supra* note 56, at 18.

[98] Classified Information Procedures Act (CIPA),18 U.S.C. app. 3 § 3 (2012).

matters and sets forth the authority by which the government may protect matters of national security."[99] The ensuing protective order must restrict access to classified information to cleared persons.[100] The defendant is not allowed to ever see the information, but his defense counsel, after having passed a security clearance, may do so.[101] CIPA also allows the government to provide a substitution or to redact sensitive information.[102]

Assuming the defendant is entitled to classified information, Section 4 of CIPA allows the government to substitute an unclassified summary or statement at the discovery stage:

> The court, upon a sufficient showing, may authorize the United States to delete specified items of classified information from documents to be made available to the defendant through discovery under the Federal Rules of Criminal Procedure, to substitute a summary of the information for such classified documents, or to substitute a statement admitting relevant facts that the classified information would tend to prove. The court may permit the United States to make a request for such authorization in the form of a written statement to be inspected by the court alone. If the court enters an order granting relief following such an ex parte showing, the entire text of the statement of the United States shall be sealed and preserved in the records of the court to be made available to the appellate court in the event of an appeal.[103]

[99] DOJ, U.S. ATTORNEYS' MANUAL, CRIMINAL RESOURCE MANUAL 2054. SYNOPSIS OF CLASSIFIED INFORMATION PROCEDURES ACT (CIPA), https://www.justice.gov/usam/criminal-resource-manual-2054-synopsis-classified-information-procedures-act-cipa (last accessed Feb. 8, 2017) [hereinafter CRIMINAL RESOURCE MANUAL 2054. SYNOPSIS OF CIPA].

[100] *Id.*

[101] *See, e.g.*, United States v. Abu Ali, 528 F.3d 210, 244-45, 254 (4th Cir. 2008) (defendant had argued that the district court's exclusion of his non-cleared defense attorney from *in camera* CIPA proceedings violated his Sixth Amendment Confrontation Clause rights. The Court ruled against him, noting that Defendant *was* represented in the hearing by other counsel *with* clearance, and finding that "[a] defendant and his counsel, if lacking in the requisite security clearance, must be excluded from hearings that determine what classified information is material and whether substitutions crafted by the government suffice to provide the defendant adequate means of presenting a defense and obtaining a fair trial").

[102] ZABEL & BENJAMIN, *supra* note 68, at 83-84.

[103] CIPA § 4.

However, if the defendant and government still do not agree on the relevance of the evidence, the defendant can then seek discovery of the classified information. The defendant must then provide notice to the government,[104] so that the government can request that the court conduct a hearing to make a determination on this issue.[105] If the judge finds after review in an *ex parte*, *in camera* proceeding that the information is not relevant to the defendant's case, the defendant is prohibited from using it at trial.[106] If the information is deemed relevant, CIPA requires that substitutions must "provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information."[107]

In CIPA cases, courts have come up with variations on the *Roviaro* standard. In *United States v. Mejia*, the Court used a three-step analysis requiring (1) that the information must be relevant, (2) that the government must have a colorable assertion of privilege, and (3) that information cannot be of mere "theoretical relevance," but must be at least "helpful to the defense."[108] Other courts have said that the classified information should be "essential to a fair determination of cause,"[109] or that it should neither be speculative nor "merely cumulative [or] corroborative."[110] One major difference in CIPA cases though is that some courts have held that even if a defendant meets the relevant and helpful threshold set by *Roviaro*, national security concerns may still win out.[111]

It is important to note that, if used in the context of NITs, CIPA would be invoked only in "outsider cases." These are cases where the defendant did not originally have access to the material and never would unless provided with it in discovery.[112] "Insider" cases are those where the defendant has already had access to the classified information, and the government will usually turn those

[104] *Id.* at § 5.

[105] *Id.* at § 6(a).

[106] TURNER & SCHULHOFER, *supra* note 56, at 19.

[107] CIPA § 6(c)(1).

[108] United States v. Mejia, 448 F.3d 436, 455-56 (D.C. Cir. 2006) (applying the test set forth in United States v. Yunis, 867 F.2d 617, 623 (D.C. Cir. 1989)).

[109] United States v. Rosen, 520 F. Supp. 2d 786, 801 (E.D. Va. 2007).

[110] United States v. Smith, 780 F.2d 1102, 1110 (4th Cir. 1985).

[111] *See, e.g.*, United States v. Rahman, 870 F. Supp. 47, 52-53 (S.D.N.Y. 1994).

[112] Ellen Yaroshefsky, *Secret Evidence Is Slowly Eroding the Adversary System: CIPA and FISA in the Courts*, 34 HOFSTRA L. REV. 1063, 1068 (2006).

documents over.[113] The "Catch-22" problem is more apparent in outsider cases, where, without already having access to the materials, defendants may not be able to effectively argue to compel that same access.[114]

D. Discovery under the Foreign Intelligence Surveillance Act (FISA)

Closely related to CIPA is the Foreign Intelligence Surveillance Act (FISA). FISA permits the government to wiretap and conduct physical searches for the purpose of gathering foreign intelligence.[115] Since the passage of the USA PATRIOT Act, FISA requests must only meet the "significant purpose" standard, meaning intelligence collection under FISA could have other purposes in addition to foreign intelligence gathering.[116] In order to use FISA material in court, the government must notify the defendant.[117] The defendant can move to suppress the evidence, but upon a filing of the "Attorney General stating that disclosure of such material would harm national security, the district court must review the FISA warrant application and related materials *in camera* and *ex parte* to determine whether the surveillance or search 'of the aggrieved person was lawfully authorized and conducted.'"[118] Courts rarely "second guess" the Attorney General's certification.[119]

In contrast to domestic wiretaps and search warrants, the government's warrant application to the Foreign Intelligence Surveillance Court ("FISC") to authorize the wiretap or search is never revealed to the defendant in the event that disclosure would detrimentally affect the United States' ability to gather foreign intelligence.[120] This premise was tested in *United States v. Daoud*, where the district judge after reviewing the classified materials granted the defendant's motion seeking access to those materials in hopes of showing that "the 'evidence obtained or derived from

[113] *Id.* at 1067-68.

[114] United States v. Yunis, 867 F.2d 617, 624 (D.C. Cir. 1989).

[115] Foreign Intelligence Surveillance Act (FISA), 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B) (2010).

[116] William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209, 1245 (2007); *see also In re* Sealed Case, 310 F.3d 717, 732-33 (FISA Ct. Rev. 2002).

[117] FISA §§ 1806(c), 1825(d).

[118] ZABEL & BENJAMIN, *supra* note 68, at 80 (quoting FISA §§ 1806(f), 1825(g)).

[119] United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984).

[120] ZABEL & BENJAMIN, *supra* note 68, at 80 (citing United States v. Rosen, 447 F. Supp. 2d 538, 546 (E.D. Va. 2006)).

such electronic surveillance' had been based on 'information [that] was unlawfully acquired' or that 'the surveillance was not made in conformity with an order of authorization or approval.'"[121] The Circuit Court overturned that ruling,[122] maintaining the practice of never disclosing FISA materials to a defendant.[123]

The *Daoud* case also demonstrates the degree to which the use of FISA has been expanded since the significant purpose standard was instituted. Adel Daoud was an eighteen-year-old American citizen when undercover FBI agents began corresponding with him online.[124] It seems troubling that courts have generally sided with the government's view that disclosure would be harmful and so have consistently blocked defendants from accessing FISA materials, regardless of defendants' age or citizenship. Prosecutions seem to now regularly rely on FISA evidence in more and more cases that have only a tangential relation to national security.

E. Problems with the Current Approach

The test used in *Roviaro* and its progeny to determine whether law enforcement privilege applied was never meant to be a bright-line rule. The Supreme Court believed that balancing the respective interests of the government's interest and the defendant called for a case-by-case review.[125] The *Roviaro* test is indeed a fact-heavy analysis, necessarily calling for judges' discretion. On the whole, this is the right approach. It makes sense to disclose a sensitive technique in a case where it is essential to determine guilt or where a technique becomes outdated and unlikely to be used again, but these are fact-dependent decisions. What seem like appropriate law enforcement tactics in one situation may not be appropriate in another.

However, uneven application of the *Roviaro* balancing test to NIT cases is potentially problematic because many cases could arise out of the same law enforcement operation. This was the issue in the Playpen Investigation cases, cases in different jurisdictions but with virtually identical facts—the only real

[121] United States v. Daoud, 755 F.3d 479, 480-81 (7th Cir. 2014) (quoting FISA § 1806(e)).

[122] *Id.* at 485.

[123] Hanni Fakhoury, *Criminal Defendants Should Have Chance to Review FISA Materials, EFF and ACLU Argue in Amicus Brief*, ELEC. FRONTIER FOUND. (May 9, 2014), https://www.eff.org/deeplinks/2014/05/new-eff-aclu-amicus-brief-argues-court-right-order-disclosure-fisa-materials.

[124] *Daoud*, 755 F.3d at 480.

[125] Roviaro v. United States, 353 U.S. 53, 62 (1957).

difference being the defendants' usernames—resulted in disparate outcomes. Whether or not a defendant succeeded on a motion to compel the entire NIT source code seems to have been wholly dependent on which judge was assigned to their case.[126] If use of NITs becomes as prevalent as its current trajectory suggests, the arbitrariness of related judicial decisions will become an even bigger problem. An already flexible *Roviaro* standard bends too far here.

Moreover, many of the crimes that NITs could target can be conducted exclusively via the computer or Internet.[127] If courts begin to veer towards compelling disclosure of NIT code, then courts are effectively forcing the government to drop criminal charges. Courts cannot mandate disclosure in situations where national security demands confidentiality and the NIT is the only viable lead that uncovered the defendant—without the NIT, the government would not have been able to identify the defendant in the first place. Until some uniform approach to NIT disclosure can be established, prosecutors will not know if they are facing the graymail problem of "disclose or dismiss" until well after they decide to begin legal proceedings.

When considering the application of CIPA to NIT exploit code, more issues with the current approach arise. One issue is that CIPA requires that defense counsel obtains security clearance.[128] As the number of NIT cases is expected to grow, it is hard to imagine that public defenders who may be assigned to NIT cases will have the time and resources to do so. Moreover, if this is the public defender's only NIT case, he may choose to forgo the trouble of obtaining security clearance, but, in doing so, he narrows the legal strategies he can pursue for his client.

Another consideration is judicial economy. Will the hundreds or even thousands of prosecutions stemming from one NIT investigation lead to individual *ex parte*, *in camera* hearings for each case as required under CIPA? Do most judges even possess

[126] *See* Part I, *infra.* Judge Bryan in the Western District of Washington seems to be particularly sympathetic to defendants' needs over those of law enforcement. *See* Joseph Cox, *Judge Rules FBI Must Reveal Malware It Used to Hack Over 1,000 Computers*, VICE (Feb. 18, 2016, 5:02 PM), https://motherboard.vice.com/en_us/article/judge-rules-fbi-must-reveal-malware-used-to-hack-over-1000-computers-playpen-jay-michaud.

[127] For example, disseminating child pornography, soliciting minors, identity theft, and criminal defamation.

[128] CRIMINAL RESOURCE MANUAL 2054. SYNOPSIS OF CIPA, *supra* note 99.

the technical knowledge to understand coding languages?[129] Perhaps looking at the actual lines of code will aid the judge in understanding the security risks involved, but it is more likely than not that the judge will not possess the requisite knowledge of computer code.[130]

IV. The New Approach: *Roviaro* 2.0

A. Lessons to Take from the Current Approach

While there are many problems with *Roviaro* as courts have currently applied it, there are three major findings that should be kept in mind when crafting a new approach.

1. Courts are increasingly integrating national security procedures into general criminal proceedings.

Cases involving national security necessitate procedures that, in a normal criminal proceeding, would seem unjust to the defendant. For example, defendants are not allowed to see the FISA warrant application,[131] and discovery hearings under CIPA are *ex parte*.[132] Cases involving the use of NITs rightly require similar measures to protect law enforcement methods and other investigations, but it is unclear if current procedures are suitable for widespread use.

Efforts to prevent leaks that may be damaging to national security could be overwhelmingly resource-intensive should more NIT-related cases arise. Defense counsel for each individual case arising out of a NIT investigation must obtain security clearances,[133] and judges in each district court must conduct *ex parte* hearings on the same issue over and over again but for different cases. Procedures like CIPA are meant to be circumspect

[129] *See, e.g.*, Caleb Garling, *Oracle Goes for Broke in Court Battle with Google*, WIRED (May 15, 2012, 9:39 PM), https://www.wired.com/2012/05/google-schmidt-page-damages/ (noting that the presiding judge had learned to code in Java in preparation for the copyright dispute over several lines of Java code).

[130] *See generally* Glyn Moody, *Should People Learn to Code? Yes – If They Are Judges Ruling on Cases Involving Software*, TECHDIRT (May 21, 2012, 3:10 AM), https://www.techdirt.com/articles/20120518/04252818965/should-people-learn-to-code-yes-if-they-are-judges-ruling-cases-involving-software.shtml (contrasting a knowledgeable judge with one who did not understand industry concerns with software patent law because of his lack of coding background).

[131] United States v. Rosen, 447 F. Supp. 2d 538, 546 (E.D. Va. 2006).

[132] Classified Information Procedures Act (CIPA),18 U.S.C. app. 3 § 4 (2012).

[133] CRIMINAL RESOURCE MANUAL 2054. SYNOPSIS OF CIPA, *supra* note 99.

at the expense of efficiency because national security is at stake, and the sensitive nature of NIT-related cases calls for similar levels of circumspection.

2. The *Roviaro* standard is heightened, but it is also flexible and context-dependent.

The "relevant and helpful" standard is harder to meet compared to the materiality threshold of Federal Rules of Criminal Procedure Rule 16. Courts will consider context when deciding whether evidence should be disclosed to the defendant, but case law has not been exhaustive on exactly which factors must be considered. The standard is necessarily flexible in order to accommodate the factual background of the case.

Indeed, the offenses charged can affect how much leeway the judicial system will give to prosecutors to present their case. For example, the right to confront witnesses can be curtailed for defendants in child abuse cases,[134] and the foreign intelligence sensitivities surrounding terrorism cases frequently prevent defendants from making a full case.[135] For cases arising out of NIT investigations, courts could be mindful of the criminal charge or charges at issue and mold their approach to the graymail problem accordingly.

3. The court may need to act as an advocate for defendants' interests.

Discovery hearings under CIPA can be *ex parte*. It is not ideal for defendants to be put in this position; the court may not view the material in a way that diligent defense counsel might.[136] However, when the defense is not present, the judge must wear two hats—that of an advocate for the defendant's point of view and that of an impartial decision-maker. These two roles can clash, but, as the discovery process stands now, judges cannot delegate one

[134] *See, e.g.*, Maryland v. Craig, 497 U.S. 836, 853 (1990).

[135] For example, in *United States v. Moussaoui*, defense counsel sought the deposition of persons in government custody for involvement in terrorism who had made statements that pointed to Moussaoui's innocence. The government argued that access would endanger national security as it would interfere with ongoing investigations. Ultimately, the court decided that access would not be granted, but that government-provided summaries of potentially exculpatory interviews or interrogations would suffice. United States v. Moussaoui, 382 F.3d 453, 476-77 (4th Cir. 2004).

[136] Yaroshefsky, *supra* note 112, at 1072.

role or the other to a third-party. As demonstrated by widespread practice of CIPA procedures, courts have accepted these dueling roles. Thus, it is vitally important that the judge be able to fully comprehend what the evidence is in order to know how that evidence may serve the defendant's purposes.

B. *What a New Approach Could Look Like*

If law enforcement is indeed moving in the direction of more frequently using NITs, both the government and the court will need to revamp how they approach NIT investigations and cases. They will need to be mindful of the sensitive, perhaps even classified, nature of NITs, the need to protect defendants' rights, and the potential burden of that mindfulness on judicial resources. An outright application of CIPA to all NIT cases is unsuitable because CIPA procedures consistently sacrifice efficiency for caution, but certain CIPA practices could and should be adopted here.

First, there should be a general presumption that law enforcement need not divulge the exploit portion of the NIT code. As in CIPA proceedings, it is generally an uphill battle for defendants to obtain access to classified material. However, the government should be compelled to turn over all other parts of the NIT code that would not aid hackers if they somehow obtained them. The method by which investigators "entered" suspects' computers is relevant evidence to the defendant, and so they should be afforded as much information as the government can give without risking national security. Evaluating only the generator, payload, and logging server should be adequate to ensure that the scope of the warrant was proper and the discovered IP address belonging to the defendant is indeed tied to the illegal activity being investigated. Perhaps courts could mandate that the government also provide a "test computer" on which the NIT operates, so that the defense could evaluate the effects of the NIT without being able to view the NIT source code. In other words, there should be a "facially legitimate and bona fide" standard that is deferential to the government regarding the NIT exploit.[137] CIPA allows the courts to fashion creative solutions to maximize both defendants' rights and the need to protect national security,

[137] *Cf.* Kerry v. Din, 135 S. Ct. 2128, 2140 (2015) (Kennedy, J., concurring) (reasoning that deference to an executive officer's decision is warranted especially in the area of national security).

and the same resourcefulness should be allowed in NIT-related cases.

Second, the presumption that law enforcement need not divulge NIT exploit code should still be limited in order to curb unnecessary government intrusions. One suggestion is that law enforcement reserve the usage of NITs for dealing with the "Four Horsemen" of the Internet—"terrorism, child pornography, drugs, and organized cyber crime."[138] This would encourage law enforcement to consider whether NITs are truly needed in smaller cases since the risk of being ordered to turn the entire code over would be greater if courts considered the necessity of NITs in its calculations. In addition, this would better justify the presumption against divulging the code as the criminal system does treat different crimes differently. For example, a defendant usually has the right to confront his accuser in the courtroom, but in child sexual abuse cases, young accusers can testify via a television screen instead.[139] This is in line with the *Roviaro* holding, where the Supreme Court mentioned "the crime charged" as a possible factor to consider.[140] This proposal simply turns "the crime charged" into a mandatory consideration.

Third, when the defendant wants to challenge the presumption of nondisclosure, courts should only allow them to do so on narrow grounds. A court would only seriously consider a defendant's motion to compel when there are concrete indications that law enforcement abused its power. For example, the court could mandate disclosure when there is a reasonable belief that the government made misrepresentations to the court regarding the limits of the NIT or the extent to which national security was at stake. If there were indications like in *Cottom* where investigators had sourced the code from a publicly accessible website,[141] then

[138] Timothy C. May, *8.3 - Anonymity and Digital Pseudonyms*, *in* THE CYPHERNOMICON: CYPHERPUNKS FAQ AND MORE 8.3.4 (1994), https://www.cypherpunks.to/faq/cyphernomicron/chapter8.html#3.

[139] *See, e.g.*, *Craig*, 497 U.S. at 837-38 (finding that Maryland's procedure for allowing a child witness to testify without seeing the defendant did not violate the Confrontation Clause of the Sixth Amendment, which the Court has read to express a "preference" for face-to-face confrontation).

[140] To decide the balance, a court would need to consider "the crime charged, the possible defenses, the possible significance of the informer's testimony, and other relevant factors." Roviaro v. United States, 353 U.S. 53, 62 (1957).

[141] United States v. Cottom, Nos. 8:13CR108; 8:15CR239, 2015 U.S. Dist. LEXIS 171880, at *6-8 (D. Neb. Dec. 22, 2015), *aff'd*, No. 16-1050, 2017 U.S. App. LEXIS 2789 (8th Cir. Feb. 17, 2017).

maintaining the secrecy of the code would not implicate national security concerns. Another scenario where defendants could challenge the presumption is if the vulnerability was patched in the intended target website or server and could not be similarly exploited against other targets.

The burden must be on the defendant to convince the court why the presumption should be challenged because abuse of power is an extraordinary allegation to make. If the government has otherwise made all efforts to cooperate in the discovery process, courts cannot simply accept allegations of abuse of power without supporting evidence. In addition to showing that the materials already turned over are inadequate, defendants must be able to show that there is a reasonable probability that the case would turn out differently had the evidence been disclosed.[142] This ensures that defendants are still able to check potential government abuse, but it also prevents the defendant from engaging in graymail and needlessly delaying proceedings.

Fourth, when multiple cases arise out of the same NIT investigation, the government should be allowed to be more creative and economical in their replies to defendants' challenges. For example, in a manner reminiscent of issue preclusion, if a law enforcement agent or expert witness has already been deposed and cross-examined on the precise issue of whether the entire NIT code needs to be divulged, the government should be able to submit a transcript of that testimony to the court without having to call the witness to court. After all, the initial deposition was theoretically conducted by another defendant who was facing the same charge, with the same interests, and targeted by the same NIT operation. If the court finds the transcript insufficient or the defendant raises plausible arguments on how his case differs, then the court can proceed with an *in camera*, *ex parte* hearing like in CIPA cases. The court should also be able to ask the government for an affidavit affirming that the NIT code at issue is still relevant to other investigations or intelligence activities in order to preempt arguments that national security is not at stake. This way, judicial resources are conserved and the same exact issue is not re-litigated over and over again.

These suggestions are meant to tighten the *Roviaro* standard only for NIT-related cases, but they could perhaps also be used to balance discovery of other sensitive law enforcement techniques—

[142] United States v. Klimavicius-Viloria, 144 F.3d 1249, 1261 (9th Cir. 1998) (quoting United States v. Bagley, 473 U.S. 667, 682 (1985)).

disclosure of which would similarly pose a genuine risk to national security. This new approach maintains the *Roviaro* standard while giving greater weight to certain factors that are already considered, such as the crime charged, when applying the standard. And while it allows for creative solutions needed in CIPA cases, this new approach would free the discovery process from the strict, resource-draining procedural mechanisms that CIPA would require for each of the thousands of NIT-related cases that are expected to arise in the future. In other words, the new approach would use a stricter *Roviaro* standard with the option to implement CIPA procedures when necessary. This tactic is more flexible than a wholescale application of CIPA to NIT-related cases but will lead to more consistent court decisions where the same facts are at issue or where one investigation leads to multiple cases in different courts.

In addition, the presumption against disclosure is better than having no presumptions at all. Because giving unchallenged access to the same full code to defendants implicated in the same NIT investigation heightens the risk of damaging national security, it is better to err on the side of withholding the full NIT code. One leak in one courtroom is enough to spread the code—known to be capable of hacking into thousands of computers—to computer-savvy wrongdoers around the world. This new approach will ensure greater uniformity across court decisions arising from the same NIT investigation, continue to respect defendants' rights, and protect security interests in an age where enforcement of general crimes increasingly implicates national security concerns.

V. Conclusion

Vulnerabilities will always exist.[143] The growing use of encryption does not change that, and NITs may be the only way for law enforcement to advance some of their investigations in the future. The change to Rule 41 of the Federal Rules of Criminal Procedure paves the way for greater use of NITs as well. Courts are ill-prepared for the rapid development happening in this area. They will need to update the current approach used to determine when law enforcement privileges apply through common law given the lack of Congressional action in this area. If a satisfactory way forward is not found, the consequences may be dire and the problem of graymailing in the digital age will only grow. The FBI and Department of Justice have already shown that they are willing to drop prosecutions in order to protect NIT source code.[144] Investigative tools have evolved alongside the growth of technology, and courts need to adapt to these changing times as well.

[143] *See* Bellovin et al., *supra* note 9, at 30.

[144] Tim Cushing, *FBI Dismisses Child Porn Prosecution After Refusing to Hand Over Details on Its Hacking Tool*, TECHDIRT (Jan. 6, 2017, 9:44 AM), https://www.techdirt.com/articles/20170106/08320436415/fbi-dismisses-child-porn-prosecution-after-refusing-to-hand-over-details-hacking-tool.shtml.