CHALLENGING GOVERNMENT HACKING IN CRIMINAL CASES
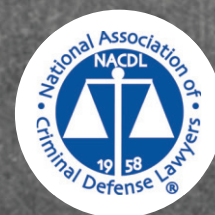
March 2017

CHALLENGING GOVERNMENT HACKING IN CRIMINAL CASES

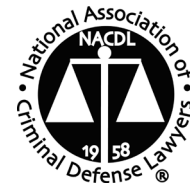
American Civil Liberties Union
125 Broad Street,
New York, NY 10004

Electronic Frontier Foundation
815 Eddy Street,
San Francisco, CA 94109

National Association of
Criminal Defense Lawyers
1660 L St. NW, 12th Floor,
Washington, D.C. 20036

Cover Image: Hugh D'Andrade

ABOUT THE AUTHORS*

AMERICAN CIVIL LIBERTIES UNION (ACLU)

For nearly 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country.

The ACLU takes up the toughest civil liberties cases and issues to defend all people from government abuse and overreach, and works to establish new privacy protections for our digital age of widespread government surveillance.

With more than 2 million members, activists, and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico, and Washington, D.C., for the principle that every individual's rights must be protected equally under the law, regardless of race, religion, gender, sexual orientation, disability, or national origin.

ELECTRONIC FRONTIER FOUNDATION (EFF)

The Electronic Frontier Foundation is the leading nonprofit organization defending civil liberties in the digital world. Founded in 1990, EFF champions user privacy, free expression, and innovation through impact litigation, policy analysis, grassroots activism, and technology development. We work to ensure that rights and freedoms are enhanced and protected as our use of technology grows.

With roughly 37,000 active donors, EFF represents technology users' interests in court cases and broader policy debates, including the debate about law enforcement "hacking." EFF has worked to educate criminal defense attorneys and the courts about the threats to privacy posed by this surveillance technique, including filing amicus briefs in seven cases arising from the Playpen investigation.

NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS (NACDL)

The National Association of Criminal Defense Lawyers is the preeminent organization in the United States advancing the goal of the criminal defense bar to ensure justice and due process for persons charged with a crime or wrongdoing. NACDL's core mission is to: Ensure justice and due process for persons accused of crime … Foster the integrity, independence and expertise of the criminal defense profession … Promote the proper and fair administration of criminal justice.

Founded in 1958, NACDL has a rich history of promoting education and reform

through steadfast support of America's criminal defense bar, amicus curiae advocacy, and myriad projects designed to safeguard due process rights and promote a rational and humane criminal justice system. NACDL's many thousands of direct members — and 90 state, local and international affiliate organizations totaling up to 40,000 members — include private criminal defense lawyers, public defenders, active U.S. military defense counsel, and law professors committed to preserving fairness in America's criminal justice system. Representing thousands of criminal defense attorneys who know firsthand the inadequacies of the current system, NACDL is recognized domestically and internationally for its expertise on criminal justice policies and best practices.

Students in the Technology Law and Policy Clinic at NYU Law School, including David Krone and Charles Low, contributed to this report.

CONTENTS

INTRODUCTION

In recent years, the government has increasingly turned to hacking as an investigative technique. Specifically, the Federal Bureau of Investigation ("FBI") has begun deploying malware: software designed to infiltrate and control, disable, or surveil a computer's use and activity. The government calls this type of hacking operation a "Network Investigative Technique," or NIT.

Law enforcement, and particularly the FBI, has been using malware to investigate online criminal activity since at least 2002.[1] While the FBI initially limited malware attacks to individual computers, it has in recent years embraced a form of bulk hacking that enables small teams of agents to hack thousands of computers in a single operation, often on the basis of a single warrant issued by a single magistrate judge.[2] The use of this controversial technique is driven in part by the increased availability and adoption of easy-to-use privacy-enhancing technologies, like Tor and Virtual Private Network ("VPN") services, which allow individuals to shield their locations and identities online, and by the use of encryption, which allows individuals to protect the contents of their communications.[3] Installing malware can enable the government to identify targets who use privacy-enabling software to hide their IP addresses, and thus their location or identity, or to access encrypted communications.

To date, the best known and most frequently litigated form of government bulk hacking is a so-called "watering hole" operation, in which the government commandeers a website associated with criminal activity, continues to operate it, and uses the site to surreptitiously deliver malware to (possibly hundreds or thousands of) computers that connect to the site. The term derives from the concept of poisoning a watering hole where certain animals are known to drink. The government can deliver the malware through a link that a user clicks on, or by programming the malware to secretly install itself on a computer once a user visits a particular page. Unbeknownst to the user, the malware then takes partial control of the computer in order to search it and send identifying information, including the computer's IP address, back to a law enforcement server.

To obtain authorization to deploy malware, the FBI uses search warrants issued by magistrate judges pursuant to Rule 41 of the Federal Rules of Criminal Procedure.[4] In several watering hole operations, the FBI has remotely searched thousands of computers located in districts around the country pursuant to *a single search warrant*—including, in the most recent known operation, searching more than 8,000 computers in 120 different countries.[5]

As of the date of publication, the legality of such government bulk hacking is being fiercely litigated in criminal cases across the country, giving rise to a quickly developing area of law. As information about law enforcement hacking has come to light, a number of federal judges have voiced concern about the legality of this technique, with some rejecting hacking warrant applications or suppressing evidence obtained by the FBI through the use of malware.

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. Such hacking has never been discussed by Congress, and we in no way endorse government hacking. However, given that the federal government is deploying malware and a recent amendment to Rule 41 only makes such deployment easier, it is our goal to ensure that all uses of malware are subject to meaningful Fourth Amendment analysis so that malware is installed only when supported by individualized suspicion. Our Fourth Amendment right to be free from unreasonable searches applies regardless of whether new technology is involved in effectuating a particular search; however, the law may be slow to catch up, particularly when the government goes to great lengths to hide details about its use of new surveillance techniques.[6] In the following sections, we explain the technologies and terminologies that surround government malware,[7] point out how to recognize the use of government malware in a criminal case, and outline the most important and potentially effective procedural and constitutional arguments that might warrant suppression of evidence.

Because, as described below, nearly every challenge to the government's use of malware to date has arisen in the context of watering hole attacks on child pornography sites, this report focuses on that context.[8] As with all new technologies, however, the government's use of malware will expand to other contexts and may be used for increasingly intrusive searches.[9] Therefore, this guide highlights good precedent and offers arguments to distinguish existing bad law and to help ensure those decisions are at least limited to the child pornography context.

CHAPTER I
MALWARE: WHAT IS IT & WHAT CAN IT DO?

Generally, the term "malware" refers to software intended to damage a computer system or to take partial control of its operation.[10] While this report focuses on law enforcement's use of malware to hack into computers in order to identify users, the term can also refer to malicious software used for other goals. In a number of recent incidents, for example, criminals have used malware known as "ransomware" to hold individuals' and organizations' data hostage and extort payment for its release.[11] In another case, "Stuxnet," a piece of malware believed to have been developed jointly by U.S. and Israeli intelligence, was designed to target and disable the Iranian nuclear weapons program.[12] Stuxnet then escaped the target system and began to damage non-target computers, highlighting both the potential reach of malware and how difficult it can be to control. Similarly, in Germany, the government infamously deployed "Bundestrojaner" (state Trojan horse), which enabled the government to "not only siphon away intimate data," but also provided a technical vulnerability through which anyone on the Internet could install or activate programs on an infected device.[13] And, in Mexico, spyware developed by an Israeli surveillance company was used to send disturbing messages from unknown numbers to targets—including nutrition advocates who had done nothing more controversial than support a soda tax—claiming that people close to them had died.[14]

The FBI relies on malware to collect information that is transmitted by or stored on anonymous targets' computers. In 2007, in one of the earliest-known cases of FBI hacking, the FBI employed a piece of malware known as a Computer Internet Protocol Address Verifier ("CIPAV") to identify an anonymous user who had posted online bomb threats about a high school in Washington State.[15] After news of the FBI's use of malware in that investigation spread, FOIA requests revealed that the FBI had been deploying CIPAVs to search anonymous users' computers since at least 2002.[16]

In the past few years, the FBI has expanded from the tailored deployment of malware against individual targets to watering hole operations, in which the FBI delivers malware to people who visit a particular website. The FBI is known to have conducted watering hole operations on at least three occasions, each targeting users of child pornography sites—most recently and expansively in a 2015 operation aimed at the "Playpen" website.[17]

TOR AND THE DARK WEB: WHAT ARE THEY & HOW DO THEY RELATE TO LAW ENFORCEMENT'S USE OF MALWARE?

In recent reported cases, malware has played a key role in the investigation of sites on the "Dark Web" and in unmasking users employing anonymity-protecting technology such as "Tor." Among other things, Tor is a network that helps to maintain the privacy and security of a user's IP address,[18] location, and usage by directing his or her online traffic through a series of relays.[19] Tor can also maintain the privacy and security of a webserver's IP address. Websites that are only accessible to visitors using Tor are colloquially known as "DarkNet" sites, "onion services," or "hidden services." Collectively, these sites may be referred to as the "Dark Web." A Tor user who visits a hidden service cannot learn the real IP address for that website's server through the act of making that connection, nor can the website learn the IP address for the user.

Using Tor to browse anonymously or connect to hidden services is relatively straightforward and does not require a high level of technical sophistication. In fact, following simple instructions, most Internet users can do it within five minutes.[20] Users need only download a special web browser known as the "Tor bundle" from the Tor Project, the U.S.-based non-profit that develops Tor.[21] After installation, the Tor browser automatically configures a Tor network connection every time the user opens the program. The Tor user can then find unique addresses for DarkNet websites by searching on the Internet or using DarkNet-specific search engines such as TORCH.[22]

Behind the scenes, of course, Tor's process of establishing an anonymous, encrypted connection is more complicated. Tor employs a series of volunteer computers or "relay nodes" to transmit the connection request.[23] When a user sends out a connection request, the original data is encrypted in such a way that only the last (or "exit") relay can decrypt it. That bundle, in turn, is encrypted in such a way that only the relay right before the exit relay can decrypt it, and so on, in layers, all the way to the first (or "entry") relay. This means that the request sent to the entry relay is bundled in as many layers of encryption as there are relays. And, as the request gets to each relay, that relay decrypts the only layer it knows how to decrypt. When the request gets to the exit relay, that relay knows to send the request to the designated server, which then sends the requested content back through the encrypted chain of

Tor relays. As a result—and most importantly—no single server in the Tor network can trace a user's path through the network to the requested site.[24]

The following graphics depict the process visually:
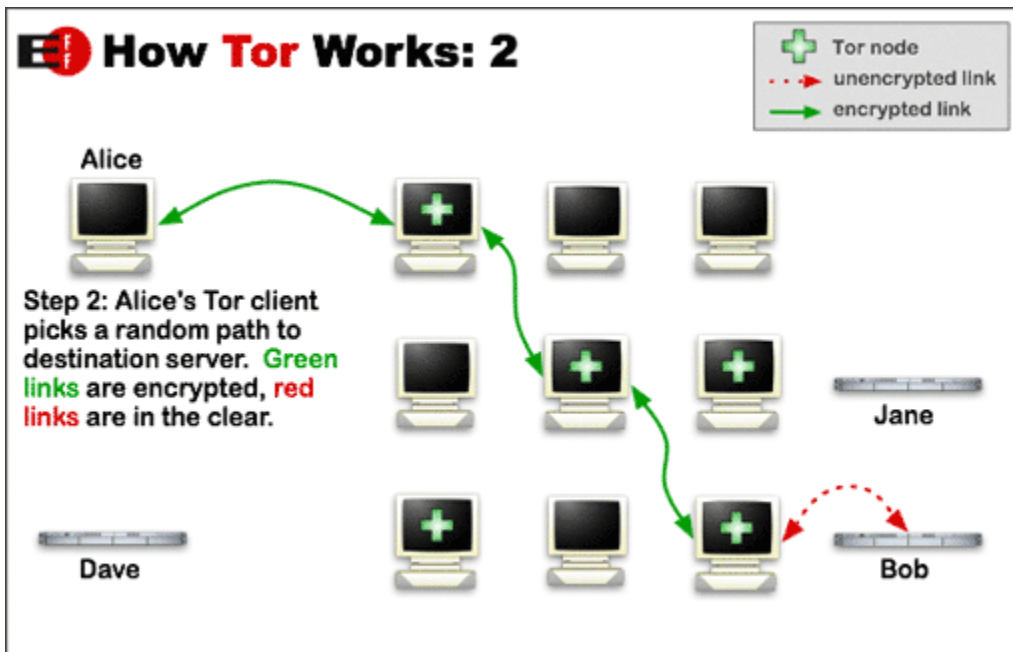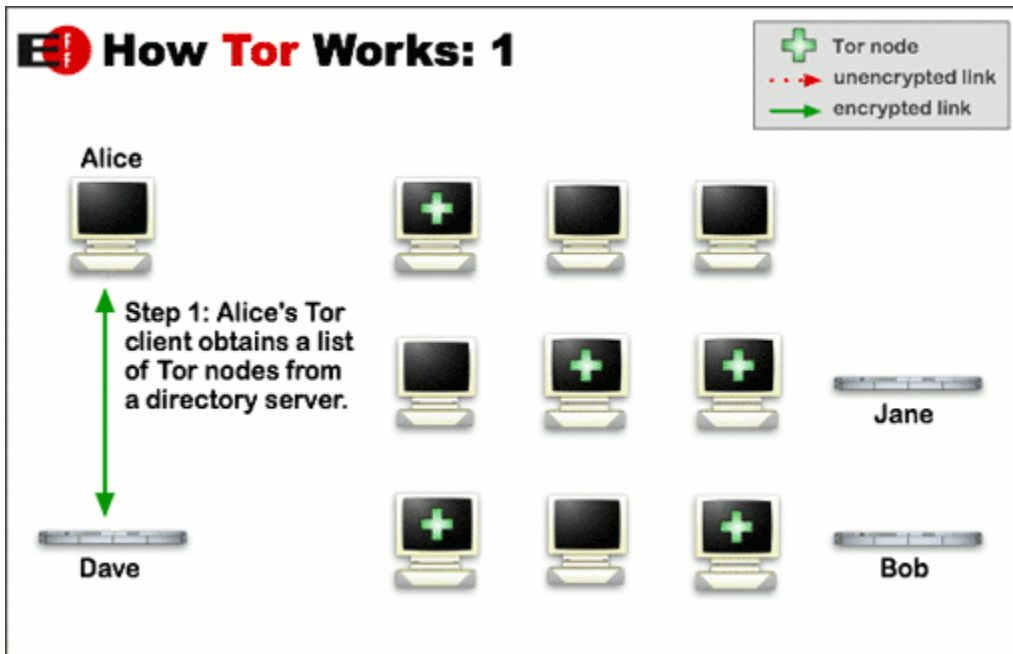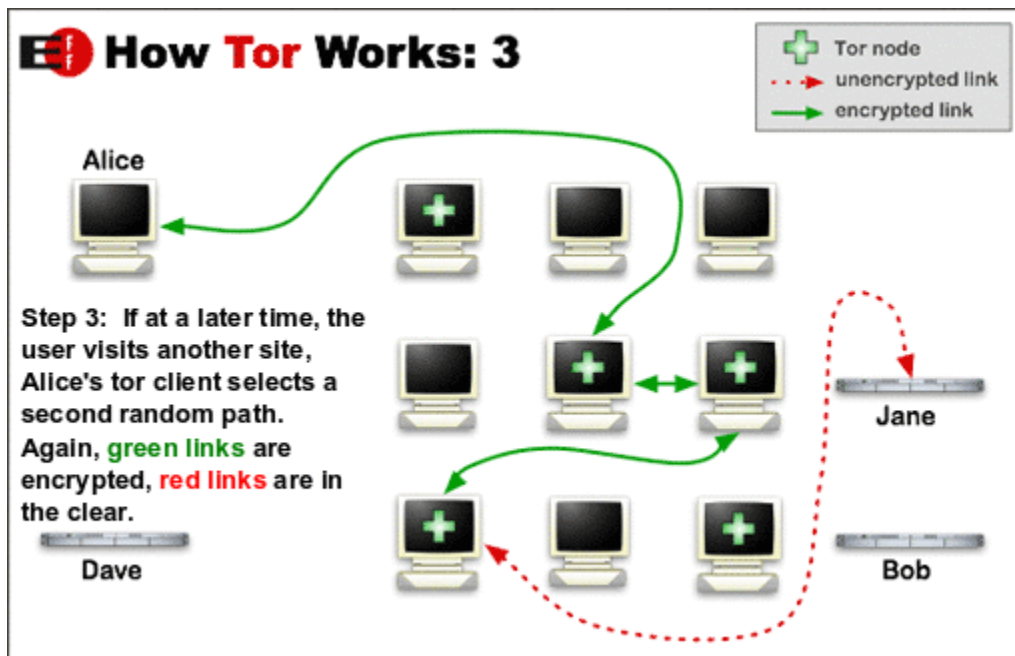
Tor serves as an essential tool for activism and free speech across the world. Journalists, bloggers, whistleblowers, human rights workers, and other activists have relied on the Tor network to avoid surveillance and other Internet controls by potentially repressive regimes.[25] Reporters Without Borders' 2015 report, "Safety Guide For Journalists," for instance, recommended that journalists concerned about surveillance use a tool where communications are "encrypted and sent over the Tor network."[26] In 2010, the State Department announced its support for the "development of new tools that enable citizens to exercise their rights of free expression by circumventing politically motivated censorship."[27]

In fact, the Tor technology was originally created by the U.S. Naval Research Lab to allow naval investigators to hide their activities online.[28] The U.S. government remains the biggest financial supporter of Tor, and the Tor Project has, in just the past few years, received millions of dollars in funding from the State Department, the National Science Foundation, and the Defense Department ("DARPA").[29]

Upon learning of websites associated with criminal activity that are often accessed via Tor, the FBI has begun requesting warrants to commandeer the sites (generally by seizing their servers) in order to deliver malware to exploit flaws in the Tor browser.[30] As noted above, the government can deliver the malware through a link that a user clicks on, or through code that secretly installs itself on a computer once a user visits a particular webpage. Once installed on an individual's computer, the malware takes advantage of a security flaw in the computer to surreptitiously take partial control of it, search it, and send identifying information back to a law enforcement server.[31]

TYPES OF INFORMATION TARGETED BY MALWARE

Once malware obtains access to a computer, there are few limits to what it can do. As described above, malware has been used to collect ransom, scare health advocates, and attempt to disarm a nuclear weapons program. Even within the realms of collecting private information and unmasking individuals, the possibilities are

essentially limitless. In one recent case, law enforcement sought a warrant authorizing the NIT malware to collect photographs, account records, and other evidence related to criminal activities from the target computer.[32] And, as noted above, existing spyware can take control of the target's camera to record live footage. As the Supreme Court recently warned in *Riley v. California*, modern computing devices are capable of storing entire warehouses' worth of information[33]—a reality that highlights the frightening potential of NIT malware.

Most frequently, law enforcement deploys malware in order to identify users who seek to anonymize themselves online. In recent cases, a single NIT warrant has allowed the FBI to collect identifying information from thousands of computers, including each computer's IP address, operating system, "MAC address" (a unique identifier assigned to each network interface), and active username (the account under which an individual user has logged onto the device).[34] Law enforcement then uses this information to tie a computer to an individual. First, with the help of the Internet Service Provider in control of the seized IP address, law enforcement uses the seized IP address to associate online behavior with a specific internet account. Law enforcement then uses the MAC address to identify a particular device connected to that account and, by determining which username was logged into that device at a specific time, law enforcement can finally link online behavior to an individual. Or law enforcement can determine a device's approximate latitude and longitude by using malware to track the device's use of wireless access points and checking those points against an external database maintained by private companies.[35] Thus, law enforcement may be able to determine the *physical* location of the computer, or to identify which particular user was likely on the computer at the time of the alleged criminal activity.

As noted briefly above, in addition to gathering information to identify the user of a computer, the government can also use NIT malware to collect other content stored on the hard drive of a target's computer or to capture user credentials for social media sites such as Facebook or Google. And the government's use of malware can spread even further—from the initially-infected device to a user's other devices, such as her smartphone or printer.[36] However, good security practices, such as the prompt installation of software updates, can make it harder for law enforcement to successfully deliver malware to remote targets.[37]

EXISTING WATERING HOLE ATTACKS

All of the known FBI watering hole operations have targeted child pornography websites. These include the "Torpedo" sting investigation in 2012, the "Freedom Hosting" sting investigation in 2013 (which also targeted TorMail, which is not a child pornography site), and the "Playpen" sting investigation in 2015.[38] Defendants continue to challenge information gathered as a result of these three investigations, and it is possible that your client's charges may be related to one of these large-scale watering hole operations, described in turn below.

In November 2012, through the Torpedo operation, the FBI seized three DarkNet sites that hosted child pornography.[39] Over the next several weeks, the FBI operated the sites, including Pedoboard, and deployed three court-authorized NITs—one on each site—to obtain the IP addresses of visitors.[40] Through Torpedo, the FBI collected IP addresses for at least 25 visitors and took at least 14 criminal defendants to trial.[41]

Each defendant moved to suppress the evidence obtained through the NIT, but a single magistrate judge denied all of the motions.[42]

In the next known bulk hacking operation, the Freedom Hosting sting, the FBI seized a group of servers in July 2013. These servers hosted various websites on the Dark Web—some, but not all, of which contained child pornography.[43] Also among the websites and services was an email service known as TorMail, which was "used by a range of people, from criminals to dissidents and journalists."[44] On August 4, 2013, the homepage of TorMail was replaced with a "down for maintenance" message; some technically sophisticated users noticed that when they visited the TorMail homepage, the website attempted to covertly deliver malware to their computers. Security researchers who subsequently analyzed the code determined that it collected identifying information about visitors to the site and then transmitted that information back to a server in Northern Virginia. The FBI later confirmed that it had deployed malware on Freedom Hosting websites after seizing the Freedom Hosting servers. The FBI initially sealed the warrant it relied upon for the 2013 operation. In response to an ACLU push to unseal the relevant case dockets, the FBI finally released the warrant and application in November 2016—revealing that the FBI had sought to hack more than 300 specific users across 23 separate websites.[45]

In the FBI's 2015 Playpen sting, part of "Operation Pacifier," the agency seized control of a server running a child pornography website referred to as "Website A," and covertly operated it from its own servers in Virginia between February 20, 2015 and March 4, 2015.[46] Court documents state that the site was devoted to child pornography and was named "Playpen."[47] The website had more than 158,000 members, and allowed members to upload or view images of their choosing.[48] According to a transcript from one evidentiary hearing, the FBI "obtained over 8,000 IP addresses, and hacked computers in 120 different countries" through the operation.[49] All of these NIT deployments were authorized by a single warrant issued by a single magistrate judge, sitting in the Eastern District of Virginia.[50] The investigation resulted in charges against at least 137 persons.[51] Given the breadth of the warrant and its deployment, the majority of the cases discussed below arose from challenges to the Playpen NIT.

CHAPTER II

HOW CAN YOU TELL IF THE GOVERNMENT USED MALWARE IN YOUR CASE?

Whenever you have a case involving charges arising from illegal online activity, you'll want to know the precise facts that gave rise to a probable cause warrant and how the government located your client. The fastest way to recognize if the government used malware in your case is to read the warrant application, affidavit, and warrant itself. In all of the malware operations known to date, the FBI's use of this technique was authorized by a search warrant issued pursuant to Rule 41.[52]

The most unequivocal sign that malware has been used is a NIT-specific warrant section titled "Court Authorized Use of Network Investigative Technique." An explicit NIT-based warrant application may describe law enforcement activity that sends communications or instructions to your client's computer in order to deliver identifying data to a government computer. Your client's computer may be referred to as a "receiving computer"—meaning one that directly receives the government's malware and instructions—or an "activating computer," meaning one that visits a particular suspect website and "activates" the malware stored there by the government. This form of data-sharing between your client's and the government's computers may also be described as "network level messaging."

But warrants may not be so forthcoming, and may indicate the use of malware in a subtler fashion. When reviewing search warrants that are turned over to you, look for references to other warrants. In addition, look out for any unexplained gaps in the chain of evidence—such as law enforcement's identification of a target's IP address or physical location purportedly based on internet activity that could not actually provide such information—and for any evidence gathered as a result of "electronic surveillance," including any mention of a particular server or website or any indication that probable cause was based on traffic to or downloads from a particular website. Because malware operations may involve an ongoing investigation, it's common for a website to have a vague identifier in a warrant application, such as "Website A" or "Bulletin Board A." NIT-based warrants may also include an explicit reference to Tor, or a generic descriptor of a service that is designed to facilitate anonymous online communication. And keep an eye out for any language indicating that a website, its server, or web-hosting facility has been "seized" or run from a new server in Virginia or Maryland, were most sites operated and servers seized by the FBI are located.

The warrant applications in *U.S. v. Michaud* provide a good example. In that case, the NIT Warrant cover sheet described the "Place to be Searched" as the computer server hosting the DarkNet website—which was located at a government facility in that district.[53] The warrant noted that "the activating [target] computers are those of any user or administrator who logs into the TARGET WEBSITE by entering a username and password."[54]

CHAPTER III
AVAILABLE DISCOVERY REQUESTS

If you believe that malware has been used in your client's case, you may be entitled to discovery designed to find out more about the NIT process. A recent case from the Ninth Circuit, although not specific to online activity or malware, reaffirms the right of criminal defendants to engage in discovery pertinent to assessing the scope of any search under the Fourth Amendment.[55] Below is a list of potential discovery requests under Rule 16,[56] which may reveal facts relevant to the legal challenges outlined below:

- All warrants, warrant applications, and any related documents that were used to identify [Client's Name], including affidavits for the seizure of any server used to deploy the NIT against the target website and the NIT warrant itself.

- The complete source code for the NIT, including the exploit and payload (this can give you or an expert valuable information about the scope and process of the search).[57]

- The amount and prevalence of illegal content hosted by or accessed on the target website, by both defendant and all other users, ideally as a percentage of all content on the target website (this information can help you assess whether probable cause exists for all users who encounter the NIT).

- The number of visitors to the target website and the number of total visits to the site [during relevant dates], by both defendant and all other users.

- The total length of time spent on the target website [during relevant dates] and the average number of hours spent on the site, by both defendant and all other users.

- Any communications on or off the target website between the [relevant government agency] and (i) defendant and (ii) other users.

- Any [agency] activity on the website during the [relevant dates], including but not limited to measures taken to monitor, collect, or block access to certain content on the target website, and other communications such as private chat messages.

Four motions to compel discovery, filed in Playpen cases, are included in Appendix C. These samples can also serve as starting points for drafting.

CHAPTER IV

AVAILABLE LEGAL ARGUMENTS

NIT warrants stretch the limits of the Fourth Amendment and the Due Process Clause. They also contravene the territorial limits on magistrate jurisdiction set forth in an earlier version of Rule 41(b), which applies to any warrant issued before December 1, 2016.[58] Defense attorneys have moved to suppress evidence obtained via NIT warrants in a number of cases in recent years—most stemming from the Playpen operation—with varying degrees of success.

The arguments for suppression are explained below. We begin with constitutional arguments in an attempt to ensure that all uses of malware are subject to meaningful Fourth Amendment analysis and in recognition of the recent change to Rule 41(b), which took effect on December 1, 2016, and will make rule-based challenges to warrants issued after that date more difficult.

FOURTH AMENDMENT ARGUMENTS

The need for a warrant in the first place depends, of course, on whether deploying a NIT on a suspect's computer is a search; if it is not a search, almost all challenges are unavailable.[59] Use of malware, unequivocally, is a search. Furthermore, the NIT's collection of information is a seizure. While some courts have held that NIT deployment is not a search, most courts agree that a warrant is indeed required.[60]

Once a court determines that a NIT deployment is a search, the following Fourth Amendment challenges are available: (1) probable cause is lacking; (2) the warrant lacks specificity; and (3) relatedly, the scope of the warrant is overbroad or the warrant functions as a "general warrant."[61] On at least one occasion a magistrate judge has declined to issue a NIT warrant on Fourth Amendment grounds[62] and, in four other cases, district judges found that the Playpen NIT warrant violated the Fourth Amendment—though they ultimately denied suppression based on the good-faith exception[63] or in light of binding circuit precedent.[64] Most recently, a magistrate judge issued a report and recommendation holding that the Playpen NIT warrant violated the Fourth Amendment and recommending that the court grant the defendant's motion to suppress because the good-faith exception does not apply.[65]

THE DEPLOYMENT OF A NIT ON A SUSPECT'S COMPUTER IS A SEARCH

Most courts addressing the threshold Fourth Amendment question agree that NIT deployment constitutes a search. Under either the *Katz* reasonable-expectation-of-privacy test[66] or the recently-revived physical-trespass test,[67] the deployment of a NIT on a suspect's computer is a search.

In deciding whether the Fourth Amendment applies, courts must consider the expectation of privacy not only in the information seized—here, IP address, MAC address, and other identifying information—but also in the place searched—here, the defendant's computer.[68] The majority of courts rightly agree that people have a reasonable expectation of privacy in their computers and that NIT deployment therefore constitutes a search. Several courts have relied on the Supreme Court's decision in *Riley*—which describes cell phones as "minicomputers" that create "a digital record of nearly every aspect of [users'] lives"—to conclude that "privacy concerns apply equally and arguably even more strongly to law enforcement's search of a laptop computer."[69] Another looked to appellate court holdings that individuals generally have a reasonable expectation of privacy in the contents of their home computers.[70] To illustrate the relevance of this determination, one court analogized to the more traditional context of searches of the home: "If a defendant writes his IP address on a piece of paper and places it in a drawer in his home, there would be no question that law enforcement would need a warrant to access that piece of paper— even accepting that the defendant had no reasonable expectation of privacy in the IP address itself."[71] The majority of courts to reach the issue have therefore held that a NIT deployment is a search.[72]

Defendants need only demonstrate a reasonable expectation of privacy in the place to be searched to trigger Fourth Amendment protections. Nevertheless, and depending on the reach and operation of the malware, there may also be a colorable argument that the defendant had a reasonable expectation of privacy in the information seized. With regard to IP addresses, most appellate courts to address the issue agree that

individuals have no reasonable expectation of privacy in their IP addresses because this metadata is disclosed to third parties during Internet browsing.[73] Most lower courts have extended this reasoning to IP addresses that are obscured by Tor because using Tor requires disclosing IP addresses to third-party Tor nodes,[74] though one Playpen court disagreed.[75] On the other hand, some courts have found that individuals maintain a reasonable expectation of privacy in other information seized by NITs, such as a MAC address.[76] In another case, a court considered the search for the target computer itself, which, as discussed above, involves the collection of indicators identifying physical location, as a search separate from the "search for digital information stored on (or generated by) that computer."[77]

A minority of courts has mistakenly concluded that a NIT deployment is not a search.[78] To reach this conclusion, some courts have simply ignored the significance of "the place to be searched" and reasoned that the disclosure of an IP address to a third party ends the inquiry.[79] One court has incorrectly concluded that any subjective expectation of privacy in a personal computer is unreasonable in light of the risk of (private) hacking.[80] Another held somewhat incoherently that the intrusion into a personal computer "does not matter" because "the IP address is not a physical component of the computer."[81] This results-driven jurisprudence is incompatible with well-settled principles of Fourth Amendment law. Such findings also suggest that including an affidavit or other expert testimony to explain how a NIT collects a computer's IP address may help your client.

If a court mistakenly concludes that the *Katz* test is not satisfied in a NIT warrant case, NITs may also be considered a search under the recently-revived property-based theory of Fourth Amendment rights, according to which "physically occup[ying] private property for the purpose of obtaining information" is a search.[82] A NIT deployment is a physical invasion of a private computer: the government sends code to the computer's memory, causing it to send information back to the government. The trespass theory is therefore an additional basis for concluding that a NIT deployment is a search.[83]

SOME COURTS HAVE HELD THAT VISITING A CHILD PORNOGRAPHY SITE SUPPLIES PROBABLE CAUSE, BUT STRONGER CHALLENGES LIE IN OTHER CONTEXTS

To date, court orders that have analyzed whether probable cause existed to issue a bulk NIT warrant have all arisen in the child pornography context and have uniformly concluded that probable cause did exist.[84] In cases involving Playpen, for example, courts have held that it was highly unlikely that "unintentional users" would "stumble onto [the site]" because the landing page contained sexually suggestive images of minors, its contents were almost exclusively child pornography, and it could not be accessed without jumping through numerous hoops—including using Tor and registering for the site.[85] As a result, courts have generally held that visiting the target site suffices to establish probable cause to believe that the individuals whose computers accessed the site had knowingly viewed or possessed child pornography—in and of itself a crime. [86]

The inference of illegal conduct is weaker, of course, if the website from which a NIT is deployed is not dedicated exclusively to hosting content that is illegal merely to view. In the Freedom Hosting operation, for example, it appears that the servers that

the government seized and operated hosted a wide array of content unrelated to child pornography, including TorMail, an anonymous email application that was used by dissidents and journalists, among others.[87] In light of the multiple purposes of TorMail, the inference of probable cause from a visit to its homepage is weaker than in Playpen cases. The probable cause inference is likely to be even weaker in cases involving offline crimes that cannot be proven by a person's presence on a given website.[88] Under such circumstances, a NIT deployment could run afoul of the bedrock principle that "a person's mere propinquity to others independently suspected of criminal activity does not, without more, give rise to probable cause to search that person."[89]

NIT WARRANTS CAN BE CHALLENGED FOR LACKING PARTICULARITY

There are two components of the Fourth Amendment particularity requirement: specificity and breadth.[90] NIT warrants authorize searches that are strikingly broad, and there are colorable particularity arguments to be raised. Indeed, the magistrate judge in *In re Warrant*—a bank-fraud case—declined to approve the NIT warrant on particularity grounds.[91] And, in the Playpen context, a district judge in Massachusetts expressed concern about the breadth of the NIT warrant before ultimately declining to reach the particularity question,[92] while a magistrate judge in Minnesota issued a report and recommendation holding that the NIT warrant violated the Fourth Amendment's particularity clause.[93]

SPECIFICITY

A warrant must state with specificity the place to be searched and the persons or things to be seized. The degree of precision required depends on the amount of information available to the government at the time of the warrant application; "[g]eneric classifications in a warrant are acceptable only when a more precise description is not possible."[94]

In the Playpen cases, the warrant failed to identify any particular user's device to search, or any particular place where a searched device would be located. One court correctly concluded that "the NIT warrant lacks particularity because it is not possible to identify with any specificity, which computers, out of all of the computers on earth, might be searched pursuant to this warrant."[95] Nevertheless, and without carefully scrutinizing the issue, nearly all courts have thus far determined that a warrant application describing the "place[s] to be searched" as the computers of users who log in to the site is constitutionally sufficient.[96] But a colorable argument can be made that the warrant failed the particularity requirement because the affidavit did not demonstrate the likelihood that the triggering condition would occur—that is, that the particular user at issue would log in to Playpen.[97] Considering the Playpen NIT, numerous courts have also noted that, though the warrant authorized a search upon log-in, the FBI did not in fact deploy the NIT until a user visited content within the site, past the homepage.[98]

Depending on the circumstances surrounding the use of the NIT and the specificity provided to describe targets in the affidavit, credible arguments may exist that more information was available to the government and should have been supplied in the warrant application. For example, in the most recent FBI operation, because the

government was operating the site, the government possessed data on the browsing habits of individual users of Playpen, such as the amount of time individuals spent on the site and the number and type of images they viewed. Including this information in the warrant may have helped the magistrate judge ensure that the computers targeted were the particular computers that had accessed illegal content.

When the location of a place is precisely what is sought through the search, the government must still describe the deployment of the NIT, the circumstances that led agents to wish to install the NIT, and the length of time for which deployment of the NIT is requested.[99] For example, the Playpen NIT described the NIT's deployment on "the server operating the Tor network child pornography website"[100] as identified by its Tor URL and specified that the NIT was to gather information only from computers "who log[ged] into the TARGET WEBSITE by entering a username and password."[101] The information to be gathered—seven specific items—was also clearly listed.[102] Most courts have found this to be sufficient, but the court that held that the Playpen warrant lacked particularity was not satisfied, rightly taking issue with the fact that the computers to be searched were not identified "until after the search ha[d] already occurred."[103]

Without even this information in the warrant, courts are likely to be troubled by the risk of infecting innocent users' computers—thereby enabling a search beyond the particular place described in the search warrant. Thus, the magistrate judge in *In re Warrant*, who considered an application for a NIT warrant to target a computer that was allegedly used for bank fraud, found particularity lacking in the application because it failed to explain how the NIT would be installed and how the government could ensure that innocent users would not be searched: "The Government's application offers nothing but indirect and conclusory assurance that its search technique will avoid infecting innocent computers or devices. . . . There may well be sufficient answers to th[is] question[], but the Government's application does not supply them."[104] In future cases, warrants that fail to explain the method of a NIT's deployment with more than conclusory assurances about privacy and effectiveness may be subject to challenge on specificity grounds.

OVERBREADTH

Defendants have also challenged NIT warrants as overly broad. Under the Fourth Amendment, the search authorized by a warrant may be "no broader than the probable cause on which it is based."[105] As a result, any search authorized by a NIT warrant must be limited to places and things that are supported by probable cause.

As NIT-based operations expand beyond the child pornography context, judges are likely to be sensitive to the possibility of searching innocent users' computers pursuant to an overbroad warrant. For example, in a situation akin to the TorMail case, where much of the website content was legal, a magistrate judge may agree that a warrant application to search "any computer that accesses the site" is too broad to satisfy the Fourth Amendment. Even a site that shows content that is illegal to purchase but not illegal to view may give judges pause. Defendants identified through visiting such sites will have to focus on distinguishing the facts of their case from the child pornography precedent, where the reasoning that visiting a child pornography site on the DarkWeb is sufficient to establish probable cause is likely stronger.

Several defendants have sought to challenge this conclusion even in the child pornography context by arguing that the NIT warrant—which, in the Playpen operation, authorized the search of tens of thousands of computers over an unlimited geographical area—was so broad that it amounted to a general warrant. Courts, however, have reasoned that the mere fact of visiting a site dedicated to child pornography establishes probable cause; the NIT was deployed from a child pornography site; and probable cause therefore extended to all "places to be searched," no matter how many there were.[106] However, it is not clear that an analogous brick-and-mortar warrant would survive judicial scrutiny—for example, it is not clear that courts would approve of a warrant that sought to search each individual who entered or left a low-income housing unit where drug dealing was known to be rampant.

There is a strong argument that a warrant authorizing the search of such a high number of personal computers—a number that is unknowable *ex ante*—poses precisely the threat that the warrant requirement was designed to avoid: "unbridled discretion [of] executive and administrative officers."[107] One judge, unfortunately, rejected this argument without explanation,[108] and another, who also rejected it, was badly irked by the comparison to general warrants.[109] But another judge, while not technically reaching the overbreadth question, strongly suggested that the breadth of the NIT deployed in the Playpen operation was unconstitutional, and was particularly troubled by the authorization to search computers in unknown locations.[110] Thus, depending on the judge, the analogy to general warrants may be helpful.

A related argument about breadth may also be available if a NIT is designed to search or seize a large amount of personal information. The Playpen NIT targeted seven specific categories of data, but NITs are capable of searching and obtaining any information a computer may contain—much of which will likely have nothing to do with the crime in question or the user of the computer who is suspected of committing the crime. Thus, the magistrate judge in *In re Warrant*, in finding the requested NIT deployment unconstitutionally overbroad, was troubled by the fact that a "computer [can be] used by family or friends uninvolved in the illegal scheme."[111] The NIT in that case was programmed to collect substantially more personal information than the Playpen NIT—including browsing history and the contents of communications[112]—and this likely explains the court's concern about the lack of privacy safeguards for third parties. Thus, in cases involving NITs that sweep up more than discrete categories of data, the lack of safeguards to protect personal information can be a viable basis for challenging a warrant.

Note also that a specific variant of this sort of challenge may be available when a NIT warrant seeks to authorize the use of a computer's built-in camera. The well-established tailoring and minimization standards that apply to video surveillance require, among other things, "a statement [in the warrant] of the steps to be taken to assure that the surveillance will be minimized to effectuate only the purposes for which the order is issued."[113] This requirement will be difficult to satisfy in malware cases, and was one of the many bases for the court's denial of a warrant application in *In re Warrant*.[114]

RULE 41(B) ARGUMENTS

Rule 41(b) of the Federal Rules of Criminal Procedure defines the territorial scope of search warrants that a magistrate judge can issue. Because the Federal Magistrates

Act ("FMA") grants magistrate judges "all powers and duties conferred or imposed . . . by law or by the Rules of Criminal Procedure," Rule 41(b) defines the territorial jurisdiction of magistrate judges.[115]

Prior to December 1, 2016, Rule 41(b) provided that "a magistrate judge with authority in the district . . . has authority to issue a warrant to search for and seize a person or property *located within the district*" unless the warrant fell within one of the exceptions enumerated in Rule 41(b)(2)–(b)(5)), described in detail below.[116] On December 1, 2016, Rule 41(b) was amended to add a new exemption, Rule 41(b)(6), which expands a magistrate judge's territorial reach for searches of "electronic storage media" if "the district where the media . . . is located has been concealed through technological means"—that is, it applies directly to NIT warrants.

Rule 41(b)(6) now provides, in full,

> [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 [the Computer Fraud and Abuse Act], the media are protected computers that have been damaged without authorization and are located in five or more districts.[117]

Because the government may still initiate prosecutions against defendants whose computers were searched subject to a warrant issued before December 1, 2016—including additional Playpen defendants—this section begins with a discussion of the most successful arguments to date under the old version of Rule 41(b).[118] The guide then turns to Rule 41(b) arguments for cases arising from warrants issued on or after December 1, 2016.

NIT WARRANTS ISSUED BEFORE DECEMBER 1, 2016

The majority of district courts to have addressed the Playpen NIT warrant have held that it violated Rule 41(b) (and, by implication, § 636(a)(1) of the FMA) by authorizing searches outside the district in which it was issued, though only five courts have ordered or recommended suppression on this basis.[119] Courts agree virtually unanimously that when a NIT is deployed on a suspect's computer, the search in question occurs on that computer and therefore within the district in which the computer is located. In *In re Warrant*, for example, the court explained that a "search takes place, not in the airy nothing of cyberspace, but in physical space with a local habitation and a name"—i.e., at the "location of the Target Computer."[120] As a result, for any search warrant issued before December 1, 2016, a search of a computer located outside the district in which the magistrate judge who issued the warrant sits violates Rule 41(b)(1) and § 636(a)(1).[121]

The exceptions enumerated in Rule 41(b)(2)–(b)(5) do not alter this conclusion. Rule 41(b)(4)—which grants magistrate judges "authority to issue a warrant to install within the district a tracking device" even if the person or property being tracked

leaves the district—is the only one that some courts have relied upon to find that NIT warrants do not violate Rule 41. Their reasoning is along the lines of: "whenever someone entered Playpen, he or she made, in computer language, 'a virtual trip' via the Internet to Virginia," where the NIT was installed. [122] However, most courts correctly recognize that a computer that is searched never travels to the district from which the NIT is deployed. As one court put it, "the Court would need to accept a version of the facts that is more Tomorrowland than truth [for subsection (b)(4) to apply]. . . . While the [malware] instructions may have resided on the Playpen server in the Eastern District of Virginia, [the defendant became] subject to the NIT only at the point when those instructions were downloaded to his computer [in another district.]"[123] And, in the words of another court, a NIT, in any event, "does not track; it searches."[124]

Subsections (b)(2), (3), and (5) are even less likely to save a NIT warrant issued for a district outside of the magistrate judge's jurisdiction; no court has found that any of these exemptions apply in NIT cases and the government has abandoned these arguments on appeal. Subsection (b)(2) grants magistrate judges authority to issue a warrant for a person or property outside the judge's district "if the person or property is located within the district when the warrant is issued." This exemption does not apply if, as in the majority of NIT cases to date, the place to be searched—the defendant's computer—is never located in that district.[125] Subsection (b)(3) lifts the territorial limit entirely in cases involving terrorism, as long as "activities related to the terrorism may have occurred" in the magistrate judge's district. Subsection (b)(5) extends the places for which a magistrate judge can issue search warrants to property located in "a United States territory, possession, or commonwealth," "a United States diplomatic or consular mission in a foreign state," and a residence and any land " used by . . . a United States diplomatic or consular mission in a foreign state." The scope of these exemptions is well delineated; they have not yet been applied, but could conceivably apply in future cases involving terrorism or computers outside the boundaries of the fifty states.[126]

Numerous courts have also considered the effect of the December 1, 2016 amendment on cases based on warrants issued before the rule change. At least five courts have inferred from the amendment that older warrants that allowed searches of places outside of the issuing magistrate's jurisdiction violated the rule because the old rule did not authorize what the amended rule expressly permits. In *Workman*, the court explicitly read the amendment to encompass "an entirely new grant of magistrate judge authority, rather than a clarification of the scope of Rule b(2) or (4)."[127] Similarly, the *Arterbury* court found that the amendment reflects the government's "aware[ness] of the problem of authorizing NIT warrants under the [then] current Rules of Criminal Procedure."[128] And in *Torres*, the court explained that the existence of the proposed amendment "bolstered" its finding that the NIT warrant violated the older version of Rule 41 because it "indicates at a minimum that there is currently ambiguity as to the state of the law."[129]

On the other hand, the argument has also backfired in multiple cases. In *Acevedo-Lemus*, for instance, the court interpreted the amendment as "a strong signal from the Supreme Court" that Rule 41 should permit the issuance of NIT warrants.[130] Similarly, in *Darby*, the court agreed with the government's claim that the amendment merely "clarif[ies] the scope of Rule 41(b)."[131] These conclusions are inconsistent with basic tenets of judicial interpretation: the amendment would serve no purpose if the old Rule authorized extra-district NIT warrants. Therefore, given the helpful precedent summarized above, the amendment is worth raising to indicate the limits of what the

old rule authorized—though it makes challenges to NIT warrants issued after December 1, 2016 harder.

NIT WARRANTS ISSUED ON OR AFTER DECEMBER 1, 2016

To date, no cases have considered a NIT warrant issued under the amended Rule. Going forward, Rule 41(b) arguments are less likely to succeed. However, the breadth of the amended rule may convince judges that the Fourth Amendment arguments outlined above are more salient now that magistrate judges are no longer even territorially limited. To the extent that courts find broad warrants problematic, they may now be more inclined to reach the constitutional issue.

ARGUMENTS FOR SUPPRESSION

Any argument for suppression based on violation of Rule 41(b) or the Fourth Amendment must overcome limitations on the availability of the exclusionary rule. These include the good-faith exception, which applies to defective warrants regardless of whether the defect is caused by violation of Rule 41 or the Fourth Amendment,[132] and the exigent circumstances exception.[133] Additional limits restrict the availability of the exclusionary rule in the Rule 41 context. And these limitations are especially difficult to surmount in child pornography cases, which form the bulk of precedent on this issue, due to judicial straining to favor the government in that context.[134]

In light of these limits, of the thirty-one Playpen cases finding a violation of Rule 41, only five courts have ordered or recommended suppression.[135] And of the six courts to find a constitutional defect in a NIT warrant that was being challenged on a suppression motion, one court recommended suppression,[136] but three courts held that suppression was not appropriate because the good-faith exception applied,[137] while another court found itself bound by Seventh Circuit precedent that denied suppression where a warrant had been issued without jurisdiction.[138] Numerous courts have similarly suggested that even if there were a constitutional violation, suppression would be unwarranted.[139]

SEEKING AND RELYING UPON A WARRANT THAT EXCEEDS A MAGISTRATE JUDGE'S JURISDICTION IS IN BAD FAITH

Under *Leon*[140] and progeny, "disputed evidence will be admitted if it was objectively reasonable for the officer executing a search warrant to have relied in good-faith on the judge's determination that there was probable cause to issue the warrant."[141] This "good-faith exception" also applies to reliance on a warrant that is defective because of a one-off mistake of fact or a clerical error.[142] Some courts have subsequently interpreted the exception to apply wherever the benefits of deterrence do not outweigh the costs.[143]

Given the breadth of the good-faith exception, four of the five courts to expressly hold that a NIT warrant—specifically, the Playpen NIT warrant—violated the Fourth Amendment nevertheless denied motions to suppress evidence based on the good-faith exception or binding circuit precedent.[144] The majority of courts that found that the same NIT warrant was issued in violation of Rule 41(b) denied motions to suppress on the same grounds. However, five courts that found Rule 41(b) violations

rejected the government's good-faith argument and granted (or recommended granting) the defendants' motions to suppress.

Levin was the first to do so, holding that "where a warrant is issued by a person lacking the requisite legal authority"—which is indeed the case when a magistrate judge violates Rule 41(b) and § 636(a)(1)—the warrant is "void at the outset [and] is akin to no warrant at all."[145] Therefore, *Levin* determined that cases "involving the application of the good-faith exception to evidence seized pursuant to a warrantless search are especially instructive" for Rule 41(b) violations.[146] The four other courts that suppressed (or recommended suppressing) evidence obtained pursuant to the Playpen NIT warrant similarly found that the good-faith exception cannot apply where the warrant is void *ab initio* (or from the start).[147] This argument will not apply to warrants issued after December 1, 2016, as such warrants will no longer exceed the jurisdiction of magistrate judges.

Even prior to the rule change—and notwithstanding that most courts agree that the government sought a warrant that the magistrate judge did not have the authority to issue at the time—most courts have nevertheless held that suppression is not proper in the child pornography context. To reach this conclusion, they have relied on the utilitarian principle—not entirely accepted, but thought to be how the Supreme Court currently conceives of the good-faith doctrine—that suppression is only warranted when the benefits of deterrence "outweigh the costs."[148] Most courts have seen suppression as a costly penalty in the child-pornography context.[149] If a defendant learns of and challenges a NIT warrant that was issued before December 1, 2016 for crimes that do not involve child victims, however, courts may be more likely to follow *Levin* and its progeny.[150]

SPECIAL LIMITS ON THE EXCLUSIONARY RULE FOR RULE 41(B) VIOLATIONS MAKE SUPPRESSION UNLIKELY ABSENT A FOURTH AMENDMENT VIOLATION

When considering whether to order suppression for a Rule 41(b) violation, further limitations apply. Again, because courts are less likely to find that Rule 41(b) has been violated on bulk-hacking warrants issued after December 1, 2016, the arguments discussed in this section are likely to apply only to cases arising from warrants issued before that date.

Courts generally distinguish between Rule-based defects that are of constitutional magnitude (also often referred to as "substantive" defects) and "all others" (referred to as "procedural," "technical," or "ministerial" defects).[151] Violations of constitutional magnitude call for suppression; procedural/technical violations do not warrant suppression unless there is evidence of prejudice to the defendant or that the violation was intentional.[152]

There is a good argument that a warrant issued in excess of a magistrate judge's jurisdiction is "substantively" defective. Each of the five courts that granted or recommended granting suppression on the basis of a Rule 41 violation agreed that the violation was substantive/constitutional because the magistrate judge exceeded her jurisdiction in approving the warrant.[153] Four of the courts found that this amounted to a substantive violation because, unlike the rest of Rule 41, Rule 41(b) "implicates substantive judicial authority" and therefore cannot be excused as a mere technical

defect.[154] Most of these courts did not directly tie the violation to the Fourth Amendment and failed to mention that, in most circuits, a "substantive" violation of Rule 41 is one that results in a violation of the defendants' constitutional rights.[155] But *Croghan* and *Carlson*, the courts that most recently suppressed or recommended suppressing evidence obtained pursuant to the Playpen NIT warrant, clearly tied this jurisdictional violation to the Fourth Amendment by highlighting that the Rule violation effectively resulted in a warrantless search, which was "presumptively unreasonable" and its fruits were therefore subject to suppression.[156] The *Ammons* court agreed that the Rule violation constituted a Fourth Amendment violation because it resulted in a warrantless search, although it ultimately denied suppression pursuant to the good-faith exception.[157] The strongest argument for suppression is therefore one that translates the jurisdictional defect, which some courts may view as substantive in its own right, into a warrantless search that clearly carries constitutional weight.

Even if a Rule 41(b) violation is "merely ministerial," it can still result in suppression when a defendant is prejudiced. In all but the Third Circuit, discussed in more detail below, courts agree that a defendant is prejudiced when "the search would not have occurred if the rule had been followed."[158] Some courts also extend this definition to cover searches that "would not have been so abrasive if the rule had been followed."[159]

There is a strong argument that the prejudice prong is satisfied in watering hole cases involving extra-district NIT deployments prior to December 1, 2016, because a jurisdictional defect in a warrant that authorizes an extra-district search is incurable.[160] (Where, by contrast, the government violates Rule 41(f) by, for example, failing to provide a defendant with a copy of the warrant, the defect is non-prejudicial because the search could still have occurred if the Rule had been followed.[161]) For this reason, multiple courts have found the prejudice prong satisfied in NIT warrant cases.[162] Furthermore, most courts to disagree are those that find the defendant had no reasonable expectation of privacy in the place or items searched—they disagree, in other words, not because they believe Rule 41(b) could have been complied with, but because they hold that a warrant was not required in the first place.[163]

In the Third Circuit, which employs a narrower test for prejudice,[164] the government's conduct must offend fundamental fairness in order for the defendant to have been prejudiced.[165] A district court in the Eastern District of Pennsylvania found no prejudice under this test in a Playpen NIT warrant case, reasoning that the agents who sought the warrant provided substantial amounts of information to the magistrate judge about the broad territorial scope of the search to be conducted, and that the Rule 41(b) violation was therefore not caused by any bad faith or obfuscation on the part of the government.[166] Other district courts in the Third Circuit are likely to reach the same conclusion.

Suppression is also available for a technical violation "when there is evidence of intentional and deliberate disregard of a provision in the Rule."[167] For reasons similar to those that have led courts to apply the good-faith exception in NIT warrant cases, suppression for intentional disregard of the Rule has almost never been found warranted. Numerous defendants have argued that the government's deliberate disregard for the old version of Rule 41 is evidenced by its awareness that a rule change was pending, but this argument has not been well received.[168] Some courts, moreover, have emphasized that the warrant affidavit in the Playpen case was candid about the geographic scope of the search to be conducted—including the fact that the NIT could be deployed on computers "wherever located"—and that even if the warrant

was invalid, its defects were therefore not due to any intentional deception by law enforcement.[169] But one court recommending granting a Playpen motion to suppress because "the constitutional defect in the execution of the NIT warrant was a creation of the Agents themselves, impermissibly expanding the scope and conducting searches outside the area in which the NIT warrant plainly limited searches to."[170]

DUE PROCESS ARGUMENTS FOR DISMISSAL OF INDICTMENT

In watering hole investigations, the government seizes servers known to be hosting websites dedicated to illegal activity—specifically, child pornography in all known bulk-hacking investigations to date—and continues to operate those illegal sites for a period of time in order to deploy NITs. Numerous Playpen defendants have argued that the indictment against them should be dismissed because the government's conduct in continuing to operate the illegal site was "so grossly shocking and so outrageous" as to violate their due process rights.[171] Dismissal of an indictment for outrageous government conduct can be warranted when the government becomes intimately involved in the commission of a crime,[172] or when government conduct causes injuries to innocent third parties.[173] In either case, the government's conduct must reach "a demonstrable level of outrageousness."[174]

Although dismissal for outrageous government conduct is rare—and defining conduct that is sufficiently extreme is "fraught with problems"[175]—the circumstances of child pornography watering hole investigations are demonstrably outrageous, and should suffice to make out a colorable claim.

The Second Circuit, in attempting to define the outer limits of the outrageous-conduct doctrine, has stated that "[i]t would be unthinkable, for example, to permit government agents to instigate robberies and beatings merely to gather evidence to convict other members of a gang of hoodlums."[176] If this example of outrageousness is so clear, then the constitutional invalidity of the Playpen operation—which caused "continuing and grievous harm" to thousands of victims[177]—is at least as clear. In fact, when the Second Circuit considered this argument in the child pornography context, though it ultimately found in favor of the government, the court highlighted that the child pornography context is different "from the usual undercover operation"—and that those differences raise "very serious concerns with respect to the rights of . . . the children Congress sought to protect in enacting the prohibitions on child pornography." The Second Circuit explained that, "in contrast to the usual sting operation, in which the Government sets up a phony drug transaction or another sort of dummy crime, the government agent in this case encouraged [the defendant] to go out and commit a *real* crime, with *real* victims, just so [the defendant] could later be arrested and prosecuted."[178]

One court considering a Playpen case similarly found it "easy to conclude that the Government acted outrageously here," though it, too, ultimately denied the defendant's motion to dismiss.[179] The court explained that the government had violated 18 U.S.C. § 3509(m), which requires that, in any criminal proceeding, child pornography "remain in the care, custody, and control of either the Government or the Court."[180] And the court highlighted that the government not only "facilitated the continued availability of . . . a site containing hundreds of child pornographic images for criminal users around the world" but also "improved [Playpen's] technical functionality," "re-victimized hundreds of children," and "used the child victims as

bait." Finally, the court noted that the government placed its lawyers at risk of violating the rules of professional conduct.[181]

Even so, the court denied the motion to dismiss for outrageous conduct after applying the multi-factor test outlined in *United States v. Black*.[182] Among other reasons for the denial, the court noted that, while the government provided the opportunity for the crimes charged, it did not create the crimes. Other decisions have followed a similar pattern, expressing discomfort[183] with the government's tactics but ultimately allowing the cases to proceed upon finding that the defendant's action was voluntary.[184]

Still others have explicitly found that the government's actions in this sting operation were not sufficiently outrageous to justify dismissal—for example, because the government purportedly "convened regularly to assess the continued benefits of the investigation," shut down the site upon deciding the benefits no longer outweighed the costs, continuously monitored postings to the site, and identified or rescued 49 children from the images Playpen.[185] But even those courts described certain aspects of the sting as "troubling."[186]

The government itself has repeatedly acknowledged that "young victims are harmed every time an image is generated, every time it is distributed, and every time it is viewed."[187] By that standard, the government repeatedly revictimized thousands of children over the two weeks that it hosted and operated the Playpen site—not only because the government enabled continued access to the site, but also because use of the site grew exponentially while the government operated it. Whereas Playpen had an average of 11,000 unique weekly visitors before February 20, 2015,[188] that number grew nearly five-fold, to approximately 50,000, while the government was operating the site.[189] The roughly 100,000 users who visited Playpen while the government was operating the site posted approximately 13,000 links to images or video files of child pornography and clicked on 67,000 unique links to child pornography images and videos—adding tens of thousands of victims.[190] And the harm resulting from the Playpen sting was caused not by tangential government involvement in an ongoing criminal enterprise, but by the government *becoming the criminal enterprise.*

This argument should apply to the government's continued operation of any illegal site following its seizure for NIT deployment: if the government believes that sufficient probable cause exists to seize the site and deploy bulk malware on visitors, its continued operation of the site must involve outrageous conduct—namely, operation of a criminal enterprise.

The *Workman* decision lends some support to this argument. Though it did not consider this due process argument, the *Workman* court rejected the government's exigent circumstances argument for similar reasons. After finding that the NIT deployment amounted to a warrantless search, the court rejected the government's argument that the exigency of the ongoing abuse of children by Playpen users justified the warrantless search because "the government manipulated the exigent circumstances by seizing the Playpen server and then running Playpen from an FBI facility for nearly two weeks."[191] There is good reason to suspect, then, that even though it is disfavored, the outrageous-conduct doctrine may provide grounds for dismissal of indictments stemming from watering hole operations.

CONCLUSION

Defense attorneys must be vigilant in raising the arguments that have gained momentum in the child pornography context—specifically, that bulk NIT warrants issued before December 1, 2016 are void because the issuing magistrate judge exceeded his or her jurisdiction—and in ensuring that courts refuse to extend the bad law created due to the specifics of child pornography to any other context. Going forward, attorneys will likely have to focus on constitutional arguments, but courts may be more willing to reach such arguments once they recognize that the limiting principle provided by Rule 41(b)'s territorial definition no longer exists.

ENDNOTES

1 Kevin Poulsen, Visit the Wrong Website, And the FBI Could End Up In Your Computer, Wired, Aug. 5, 2014, http://www.wired.com/2014/08/operation_torpedo [hereinafter Poulsen, Visit the Wrong Website].

2 Jessica Conditt, FBI hacked the Dark Web to bust 1,500 pedophiles, Engadget, Jan. 7, 2016, http://www.engadget.com/2016/01/07/fbi-hacked-the-dark-web-to-bust-1-500-pedophiles.

3 See Ryan De Souza, FBI Randomly Used Malware on TORMail Users While Busting Pedophiles, Hackread, Jan. 24, 2016, https://www.hackread.com/fbi-hacked-tormail-users.

4 As discussed in detail in Chapter IV, most known malware warrants were issued pursuant to a version of Rule 41 that has recently been amended in ways that are likely to impact the success of Rule 41-based challenges to future malware warrants.

5 Joseph Cox, The FBI Hacked Over 8,000 Computers In 120 Countries Based on One Warrant, Motherboard, Nov. 22, 2016, https://motherboard.vice.com/read/fbi-hacked-over-8000-computers-in-120-countries-based-on-one-warrant [hereinafter Cox, FBI Hacked Over 8,000 Computers] (citing Hearing Transcript in United States v. Tippens, No. Cr16-5110RJB (W.D. Wash. Nov. 1, 2016)).

6 Stephanie Pell and Christopher Soghoian, A Lot More than a Pen Register, and Less than a Wiretap, 16 Yale J. L. & Tech. 1, 134 (2013) http://digitalcommons.law.yale.edu/cgi/view content.cgi?article=1102&context=yjolt.

7 You may have already noticed several terms that you are unfamiliar with. Whenever this is the case, please refer to our glossary, located in Appendix A. For a summary of the NIT warrant cases cited in this guide, please refer to Appendix B.

8 David Bisson, FBI Used Metasploit Hacking Tool in 'Operation Torpedo', Tripwire, Dec. 16, 2014, http://tripwire.me/29efAEC; Joseph Cox, The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers, Motherboard, Jan. 5, 2016, http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers [hereinafter Cox, FBI's 'Unprecedented' Hacking].

9   There have already been cases in which law enforcement deployed malware for other purposes, such as seizing data on a user's computer or using a webcam to surreptitiously capture pictures of a target. See In re Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 756 (S.D. Tex. 2013).

10   Malware, Dictionary.com, http://www.dictionary.com/browse/malware (last visited Jan. 9, 2017). The term is formally defined by the U.S. National Institute of Standards and Technology as "a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system." Murugiah Souppaya and Karen Scarfone, Guide to Malware Incident Prevention and Handling for Desktops and Laptops, Nat'l Inst. of Standards and Tech. Special Publication (2013), http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-83r1.pdf.

11   Sean Gallagher, Patients diverted to other hospitals after ransomware locks down key software, Ars Technica, Feb. 17, 2016, http://arstechnica.com/security/2016/02/la-hospital-latest-victim-of-targeted-crypto-ransomware-attack/.

12   Nate Anderson, Confirmed: US and Israel created Stuxnet, lost control of it, Ars Technica, June 1, 2012, http://arstechnica.com/tech-policy/2012/06/confirmed-us-israel-created-stuxnet-lost-control-of-it/.

13   Glyn Moody, German police can now use spyware to monitor suspects, Ars Technica, Feb. 25, 2016, https://arstechnica.com/tech-policy/2016/02/german-police-can-now-use-spying-malware-to-monitor-suspects/.

14   Nicole Perlroth, Spyware's Odd Targets: Backers of Mexico's Soda Tax, N.Y. Times, Feb. 11, 2017, https://www.nytimes.com/2017/02/11/technology/hack-mexico-soda-tax-advocates.html.

15   Nate Anderson, FBI uses spyware to bust bomb threat hoaxster, Ars Technica, July 18, 2007, http://arstechnica.com/security/2007/07/fbi-uses-virus-to-bust-bomb-threat-hoaxster/.

16   Kevin Poulsen, Documents: FBI Spyware Has Been Snaring Extortionists, Hackers For Years, Wired, April 16, 2009, https://www.wired.com/2009/04/fbi-spyware-pro/.

17   Cyrus Farivar, After FBI briefly ran Tor-hidden child-porn site, investigations went global, Ars Technica, Jan. 22, 2016, http://arstechnica.com/tech-policy/2016/01/after-fbi-briefly-ran-tor-hidden-child-porn-site-investigations-went-global/.

18   An IP address is a string of zeros and ones that identifies a machine that is connected to the Internet, and which is used to route messages to that machine. Unlike a "MAC" address, which, as described further below, is unique and static, an IP address is not permanent and one machine could have more than one IP address over its lifetime—or even at a given time. See also Why Does Your IP Address Change Now and Then?, WhatIsMyIPAddress.com, http://whatismyipaddress.com/keeps-changing (last visited Jan. 9, 2017).

19   According to the Tor Project, the U.S.-based non-profit that develops Tor, "[t]he entire purpose of the network is to enable users to communicate privately and securely." Statement from the Tor Project re: the Court's February 23 Order in U.S. v. Farrell, Tor Project (Feb. 24, 2016) https://blog.torproject.org/blog/statement-tor-project-re-courts-february-23-order-us-v-farrell.

20   Chris Campbell, Access the Dark Web in 5 Minutes or Less, Laissez Faire Today, Mar. 1, 2016, http://lfb.org/access-the-dark-web-in-5-minutes-or-less/.

21   What is Tor Browser?, Tor Project, https://www.torproject.org/projects/torbrowser. html.en (last visited Jan. 9, 2017). More advanced users can download a Linux-based operating system known as "Tails" that has more features. Tails, https://tails.boum.org/ (last visited Jan. 9, 2017).

22   Hidden service host names are listed as a string of numbers and letters with the suffix ".onion." For instance, "xmh57jrzrnw6insl.onion" is the host name for TORCH, the DarkNet search engine.

23   In fact, Tor was initially known as "The Onion Router," alluding to the multiple layers involved in making any connection request.

24   Tor: Overview, Tor Project, https://www.torproject.org/about/overview.html.en (last visited Jan. 9, 2017).

25   Users of Tor, Tor Project, https://www.torproject.org/about/torusers.html.en (last visited Jan. 9, 2017).

26   Safety Guide for Journalists, Reporters Without Borders (2015) https://rsf.org/sites/default/files/guide_journaliste_rsf_2015_en_0.pdf.

27   Hillary Clinton, Sec'y of State, Remarks on Internet Freedom, Jan. 21, 2010, http://www.state.gov/secretary/20092013clinton/rm/2010/01/135519.htm.

28   Yasha Levine, Almost Everyone Involved in Developing Tor was (or is) Funded by the US Government, Pando, July 16, 2014, https://pando.com/2014/07/16/tor-spooks/; see also Our Sponsors, Onion Routing, https://www.onion-router.net/Sponsors.html (last visited Jan. 9, 2017); United States v. Knowles, No. CR 2:15-875-RMG, 2016 WL 6952109, at *2 (D.S.C. Sept. 14, 2016) ("The Department of Defense designed Tor to protect government communications").

29   Alex Hern, US government increases funding for Tor, giving $1.8m in 2013, Guardian, July 29 2014, https://www.theguardian.com/technology/2014/jul/29/us-government-funding-tor-18m-onion-router; see also Tor: Sponsors, Tor Project, https://www.torproject.org/about/sponsors.html.en (last visited Jan. 9, 2017).

30   Because browsers are complicated programs, they can be exploited in various ways, resulting in varying degrees of damage—as shown by the examples provided in the beginning of Chapter I. Even the lowest form of damage, known as a "minor sandbox break," can reveal a device's IP address. A minor sandbox break occurs when malware convinces a browser to go outside of its usual, contained environment. For example, such malware can pull information—including a device's IP address—by forcing the device to connect through the device's non-Tor connection when, if functioning properly, the browser would rely on Tor. The specific way in which the malware forces the browser to malfunction is called an "exploit," while the directions regarding what the malware wants the browser to do is called a "payload."

31   See, e.g., Knowles, 2016 WL 6952109, at *4–5 (D.S.C. Sept. 14, 2016); United States v. Cottom, No. 8:13CR108, 2015 WL 9308226, at *2 (D. Neb. Dec. 22, 2015).

32   In re Warrant, 958 F. Supp. 2d at 755–56.

33   Riley v. California, 134 S. Ct. 2473, 2489 (2014).

34   See, e.g., United States v. Michaud, No. 3:15-CR-05351-RJB, 2016 WL 337263, at *2 (W.D. Wash. Jan. 28, 2016).

35   See In re Warrant, 958 F. Supp. 2d at 756. For an example of how this is done, check out Google's primer on Geolocation. The Google Maps Geolocation API, Google, https://developers.google.com/maps/documentation/geolocation/intro#overview (last visited Jan. 9, 2017).

36   Even for the FBI, hacking into a user's computer is an expensive and unreliable way of obtaining the user's data. See Jenna McLaughlin, The Big Secret That Makes the FBI's Anti-Encryption Campaign A Big Lie, The Intercept, Sep. 28, 2015, https://theintercept.com/2015/09/28/hacking ("compared to say the 'installation of global wiretapping capabilities in the infrastructure,' hacking is 'significantly more difficult—more labor intensive, more expensive, and more logistically complex'—which makes it harder to

conduct 'against all members of a large population.'") (quoting Steven M. Bellovin et al., Lawful Hacking: Using Existing Vulnerabilities for Wiretapping on the Internet, 12 NW. J. Tech. & Intell. Prop. 1, 64 (2014)).

37   While good security practices cannot protect users against zero-day exploits, government malware attacks often exploit older vulnerabilities that can be avoided through software updates. In addition, Tor recently released a new beta version that automatically prompts users to install any updates to Tor Messenger or Browser, making such updates even easier for the user. See Tor Messenger 0.3.0b1 is released, Tor Project (Nov. 22, 2016) https://blog.torproject.org/blog/tor-messenger-030b1-released.

38   This guide summarizes the majority of rulings on motions to suppress and motions to dismiss that have arisen from the Playpen sting through March 28, 2017, but the guide is not comprehensive and may not include all such court orders.

39   Poulsen, Visit the Wrong Website, supra note 1.

40   Id.; see also United States v. Laurita, 8:13CR107, 2016 WL 4179365, at *3 (D. Neb. Aug. 5, 2016).

41   Poulsen, Visit the Wrong Website, supra note 1.

42   Laurita, 2016 WL 4179365, at *6; Cottom, 2015 WL 9308226, at *8; United States v. Reibert, No. 13 Cr 107, 2015 WL 366716, at *7 (D. Neb. Jan. 27, 2015); United States v. Pierce, No. 13 Cr 106–108, 2014 WL 5173035, at *6 (D. Neb. Oct. 14, 2014).

43   Kevin Poulsen, FBI Admits It Controlled Tor Servers Behind Mass Malware Attack, Wired, Sept. 13, 2013, https://www.wired.com/2013/09/freedom-hosting-fbi [hereinafter Poulsen, FBI Admits].

44   Ellen Nakashima, This is how the government is catching people who use child porn sites, Wash. Post, Jan. 21, 2016, http://wpo.st/_lRh1.

45   Joseph Cox, Unsealed Court Docs Show FBI Used Malware Like 'A Grenade', Motherboard, Nov. 7, 2016, http://motherboard.vice.com/read/unsealed-court-docs-show-fbi-used-malware-like-a-grenade; see also In re Sealed Docket Sheet Associated with Malware Warrant Issued on July 22, 2013, 1:16-cv-03029-JKB (D. Md.).

46   Knowles, 2016 WL 6952109, at *5.

47   Cox, FBI's 'Unprecedented' Hacking, supra note 8.

48   See United States v. Matish, 193 F. Supp. 3d 585, 594 (E.D. Va. 2016).

49   Cox, FBI Hacked Over 8,000 Computers, supra note 5.

50   See, e.g., United States v. Levin, 186 F. Supp. 3d 26, 30 (D. Mass. 2016).

51   Knowles, 2016 WL 6952109, at *5.

52   See, e.g., Proposed Exhibit List Exhibit 101, United States v. Cottom, No. 13-cr-108 (D. Neb. April 16, 2014), ECF No. 122-1; Application and Affidavit for Search Warrant, United States v. Network Investigative Technique, No. 12-sw-5685 (D. Col. October 9, 2012), ECF No. 1; Application for Search Warrant, United States v. Myspace account "Timberlinebombinfo," No. 07-mj-5114 (W.D. Wash. June 12, 2007), ECF No. 1.

53   Michaud, 2016 WL 337263, at *2.

54   Id.

55   United States v. Soto–Zuniga, 837 F.3d 992, 1001 (9th Cir. 2016) ("our post-Armstrong case law within the Ninth Circuit indicates that Rule 16(a)(1)(E) permits discovery related to the constitutionality of a search or seizure.").

56   Rule 16 of the Federal Rules of Criminal Procedure governs discovery requests.

57   Seeking the NIT's source code can result in suppression of all fruits from the NIT warrant and dismissal of the entire case. In Michaud, for example, the defendant sought the source code and, after the government refused to turn it over, the defendant successfully moved to compel disclosure. The government refused to comply, leading the court to suppress "evidence of the NIT, the search warrant issued based on the NIT, and the fruits of that warrant." Order Denying Dismissal and Excluding Evidence, United States v. Michaud, No. 3:15-cr-5351-RJB-1 (W.D. Wash. Jan. 22, 2016), ECF No. 212. (A similar argument led the same judge to dismiss several counts in Tippens. See Order on Government's Motion Seeking Clarification of This Court's Order Dismissing Counts 1 and 3 of the Superseding Indictment, United States v. Tippens, No. CR16-5110 RJB (W.D. Wash. Mar. 16, 2017), ECF No. 180.) In Michaud, the government then moved for, and the court granted, dismissal without prejudice because "[t]he suppression order . . . has deprived the government of the evidence needed to establish Defendant['s] guilt" and because "the government remains unwilling to disclose certain discovery related to the FBI's deployment of [the Playpen NIT]." Government's Unopposed Motion to Dismiss Indictment Without Prejudice, United States v. Michaud, No. 3:15-cr-5351-RJB-1 (W.D. Wash. Mar. 3, 2017), ECF No. 227.

One persuasive argument for the defendant's need to access the source code is that the defendant cannot assess the reasonableness of the warrant otherwise. On the other hand, the government has also successfully battled motions to compel disclosure of the full source code. See Matish, 193 F. Supp. 3d at 601; Memorandum Opinion and Order Denying First Motion to Suppress, Second Motion to Suppress, and First Motion to Compel at 21–24, United States v. McLamb, No. 2:16cr92 (E.D. Va. Nov. 28, 2016), ECF No. 41 [hereinafter McLamb Order]. And in at least one case where the government failed to even preserve the source code, the court nevertheless denied a motion to suppress the information the NIT gathered. Cottom, 2015 WL 9308226, at *8.

58   This guide focuses on federal law, but other arguments may be available under state law.

59   See, e.g., United States v. Darby, 190 F. Supp. 3d 529, 527–28 (E.D. Va. 2016) ("If the use of the NIT was not a search, the Fourth Amendment was not implicated, no warrant was required, and any violation of Rule 41(b) [was] irrelevant.").

60   See, e.g., United States v. Workman, -- F. Supp. 3d ---, 2016 WL 5791209, at *6 (D. Co. Sept. 6, 2016) (a search); United States v. Adams, No. 6:16-cr-11-Orl-40GJK, 2016 WL 4212079, at *4 (M.D. Fla. Aug. 10, 2016) (same). But see Matish, 193 F. Supp. 3d at 614–22 (not a search).

61   If law enforcement collects information beyond that which is described in the warrant—login details for Gmail or Facebook, for example—it may also be possible to argue that the search exceeded the scope of the warrant.

62   See In re Warrant, 958 F. Supp. 2d at 758–61.

63   United States v. Scarbrough, No. 3:16-CR-035, 2016 WL 5900152, at *1 (E.D. Tenn. Oct. 11, 2016); United States v. Broy, -- F. Supp. 3d ---, 2016 WL 5172853, at *8 (C.D. Ill. Sept. 21, 2016); United States v. Ammons, -- F. Supp. 3d ---, 2016 WL 4926438, at *8–9 (W.D. Ky. Sep. 14, 2016).

64   United States v. Owens, No. 16-CR-38-JPS, 2016 WL 7053195, at *7 (E.D. Wis. Dec. 5, 2016).

65   Report and Recommendation at 23–30, United States v. Carlson, No. 0:16-cr-00317-JRT-FLN (D. Minn. Mar. 23, 2017), ECF No. 44 [hereinafter Carlson R&R].

66   See Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

67 See United States v. Jones, 565 U.S. 400, 404–12 (2012); see also, e.g., United States v. Acevedo-Lemus, No. SACR 15-00137-CJC, 2016 WL 4208436, at *4–6 (C.D. Cal. Aug. 8, 2016) (ignoring the trespass test).

68 See United States v. Dzwonczyk, No. 4:15-CR-3134, 2016 WL 7428390, at *10 (D. Neb. Dec. 23, 2016) ("[T]he Fourth Amendment inquiry requires an analysis not only of the information obtained, but more fundamentally, the means of obtaining it. To this end, and as applied to the facts of this case, the question is two-fold: (1) whether the defendant had a reasonable expectation of privacy in his IP address, and (2) whether he had a reasonable expectation of privacy in the location where the IP was ultimately discovered—that is, his home computer."); Broy, 2016 WL 5172853, at *4 ("Whether [defendant] had a reasonable expectation of privacy in his computer and its contents is equally as important as whether he had one in his IP address.").

69 United States v. Hammond, No. 16-CR-00102-JD-1, 2016 WL 7157762, at *2 (N.D. Cal. Dec. 8, 2016) (citing Riley, 134 S. Ct. at 2489–90); see also United States v. Kahler, No. 16-cr-20551, 2017 WL 586707, at *6–7 (E.D. Mich. Feb. 14, 2017) (additionally noting that "Internet use pervades modern life").

70 Knowles, 2016 WL 6952109, at *8 (citing string of appellate court decisions holding that "[i]ndividuals generally have a reasonable expectation of privacy in the contents of their home computers").

71 United States v. Croghan, -- F. Supp. 3d ---, 2016 WL 4992105, at *7 (S.D. Iowa Sept. 19, 2016); see also Adams, 2016 WL 4212079, at *4 ("For example, a defendant has an expectation of privacy in his garage, even if that defendant lacks an expectation of privacy in the stolen vehicle parked in the garage.").

72 See, e.g., United States v. Anzalone, -- F. Supp. 3d ---, 2016 WL 5339723, at *6 (D. Mass. Sept. 22, 2016) [hereinafter Anzalone I]; Croghan, 2016 WL 4992105, at *7; Ammons, 2016 WL 4926438, at *4; United States v. Torres, No. 5:16-CR-285-DAE, 2016 WL 4821223, at *3 (W.D. Tex. Sept. 9, 2016); Workman, 2016 WL 5791209, at * 6; Adams, 2016 WL 4212079, at *4; Darby, 190 F. Supp. 3d at 529–30, at *6; Report and Recommendation at 23, United States v. Arterbury, No. 4:15-cr-00182-JHP (D. Okla. Apr. 25, 2016), ECF No. 42 [hereinafter Arterbury R&R]; see also Order Affirming and Adopting the Report and Recommendation of the United States Magistrate Judge at 1, United States v. Arterbury, No. 4:15-cr-00182-JHP (D. Okla. May 12, 2016), ECF No. 47.

73 See, e.g., United States v. Christie, 624 F.3d 558, 573–74 (3d Cir. 2010); United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2007).

74 See Matish, 193 F. Supp. 3d at 615 ("Even an Internet user who employs the Tor network in an attempt to mask his or her IP address lacks a reasonable expectation of privacy in his or her IP address."); United States v. Farrell, No. CR15-029 RAJ, 2016 WL 705197, at *2 (W.D. Wash. Feb. 23, 2016) (Tor users "must disclose information, including their IP addresses, to unknown individuals running Tor nodes.").

75 Kahler, 2017 WL 586707, at *7 ("If a user who has taken special precautions to hide his IP address does not suffer a Fourth Amendment violation when a law enforcement officer compels his computer to disclose the IP address, the operating system, the operating system username, and other identifying information, then it is difficult to imagine any kind of online activity which is protected by the Fourth Amendment.").

76 Knowles, 2016 WL 6952109, at *8; see also United States v. Brooks, No. 16-CR-6028L, 2016 WL 7409852, at *12 (W.D.N.Y. Dec. 22, 2016) (declining to reach Fourth Amendment question until additional briefing and evidence were provided regarding expectation of privacy, including whether, "[s]imilar to the IP address[,] . . . the other data that was obtained through use of the NIT [is] the type of data that is typically conveyed by computer users to third parties or accessible by the public").

77 In re Warrant, 958 F. Supp. 2d at 757.

78   See, e.g., United States v. Henderson, No. 15-cr-00565-WHO-1, 2016 WL 4549108, at *5 (N.D. Cal. Sept. 1, 2016); Acevedo-Lemus, 2016 WL 4208436, at *4–6; Matish, 193 F. Supp. 3d at 614–22; United States v. Werdene, 188 F. Supp. 3d 431, 443–46 (E.D. Pa. 2016).

79   See, e.g., Henderson, 2016 WL 4549108, at *5; Order and Reasons at 17–19, United States v. Rivera, No. 2:15-cr-00266-CJB-KWR (E.D. La. July 20, 2016), ECF No. 69 [hereinafter Rivera Order]; Werdene, 188 F. Supp. 3d 431 at 444–45.

80   See Matish, 193 F. Supp. 3d at 619 ("[I]n today's digital world, it appears to be a virtual certainty that computers accessing the Internet can—and eventually will—be hacked.").

81   Acevedo-Lemus, 2016 WL 4208436, at *4–5; see also Matish, 193 F. Supp. 3d at 617 ("As the Court understands it, Defendant's IP address was not located on his computer . . . [it] was revealed in transit . . .").

82   Grady v. North Carolina, 135 S. Ct. 1368, 1370 (2015) (per curiam) (quoting Jones, 565 U.S. at 404).

83   See, e.g., Brooks, 2016 WL 7409852, at *11 (directing parties to file supplemental briefs "addressing whether deployment of the NIT constituted a trespass within the meaning of the Fourth Amendment").

84   See United States v. Eure, No. 2:16cr43, 2016 WL 4059663, at *7 (E.D. Va. July 28, 2016); Matish, 193 F. Supp. 3d at 603; Darby, 190 F. Supp. 3d at 530–33; United States v. Epich, No. 15-CR-163-PP, 2016 WL 953269, at *1–2 (E.D. Wis. Mar. 14, 2016); Michaud, 2016 WL 337263, at *8.

85   Epich, 2016 WL 953269, at *1; see also Darby, 190 F. Supp. 3d at 532 ("Defendant fails to explain why someone would go to the trouble of entering the Tor network, locating Playpen, registering for the site, and then logging into the site if they were not looking for illegal content."). But see Kahler, 2017 WL 586707, at *6 ("Although the individuals accessing Playpen to view child pornography were using the Tor software for heinous purposes, the software could also be used for legitimate purposes . . . a desire for online anonymity is neither unreasonable nor suspicious.").

86   A particularly unfruitful variation of the probable cause challenge is that the triggering event specified in the NIT warrant never occurred. NIT warrants are anticipatory warrants in that they prospectively authorize searches when visitors arrive at the webpage from which the NIT is launched. See Matish, 193 F. Supp. 3d at 609; see also United States v. Grubbs, 547 U.S. 90, 94 (2006) ("An anticipatory warrant is a warrant based upon an affidavit showing probable cause that at some future time (but not presently) certain evidence of crime will be located at a specified place.") (quotation marks and citation omitted). Anticipatory search warrants are not categorically unconstitutional, but they do generally assume that some condition will occur before the search is authorized. See Grubbs, 547 U.S. at 94–97.

      Multiple Playpen defendants have argued that the triggering condition in the NIT warrant was a visit to the Playpen homepage, and that this event—a prerequisite for probable cause—never occurred because Playpen changed its homepage after the warrant affidavit was executed and before the defendants visited it. See, e.g., United States v. Deichert, No. 5:16-CR-201-FL-1, 2017 WL 398370, at *5 (E.D.N.C. Jan. 28, 2017); Eure, 2016 WL 4059663, at *6; Matish, 193 F. Supp. 3d at 610; Darby, 190 F. Supp. 3d at 534. This claim has been rejected on the ground that the change to Playpen's homepage was de minimis and therefore did not obviate the existence of probable cause: the new homepage contained a different image, but that image was suggestive of child pornography content. See Eure, 2016 WL 4059663, at *7 (rejecting the anticipatory warrant argument); Matish, 193 F. Supp. 3d at 609–10 (same); Darby, 190 F. Supp. 3d at 534 (same). Note also that some Playpen defendants have sought a Franks hearing on whether the inaccuracies in the warrant affidavit regarding the Playpen homepage were made knowingly and intentionally, and that this claim has also been uniformly rejected on the ground that the homepage change was immaterial. See Eure, 2016 WL 4059663, at *7; Matish, 193 F. Supp. 3d at 604–07; Darby, 190 F. Supp. 3d at 533–34.

87   See Nakashima, supra note 44; Poulsen, FBI Admits, supra note 43.

88   In the past, NITs have been used in cases involving bank fraud and bomb threats. See In re Warrant, 958 F. Supp. 2d at 753; Kevin Poulsen, FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats, Wired, July 18, 2007, http://www.wired.com/2007/07/fbi-spyware. It does not appear that any such case has yet addressed the question of whether there was probable cause supporting the NIT warrant in that context.

89   Ybarra v. Illinois, 444 U.S. 85, 91 (1979); see also United States v. Coreas, 419 F.3d 151, 156 (2d Cir. 2005) (holding that under Ybarra, the act of logging on to a multi-purpose website is not enough to establish probable cause); cf. Dancy v. McGinley, 843 F.3d 93, 109 (2d Cir. 2016) ("[M]ere presence near someone who somewhat matches a vague description is not a reasonable basis for suspicion.").

90   See, e.g., Michaud, 2016 WL 337263, at *4.

91   In re Warrant, 958 F. Supp. 2d at 758–59.

92   Levin, 186 F. Supp. 3d at 44.

93   Report and Recommendation at 23–26, United States v. Carlson, No. 0:16-cr-00317-JRT-FLN (D. Minn. Mar. 23, 2017), ECF No. 44 [hereinafter Carlson R&R].

94   United States v. Cardwell, 680 F.2d 75, 78 (9th Cir. 1982) (citation omitted).

95   Carlson R&R, supra note 93, at 23.

96   Matish, 193 F. Supp. 3d at 608–09; Epich, 2016 WL 953269, at *2; Opinion & Order at 18, United States v. Stamper, No. 1:15cr109 (S.D. Oh. Feb. 19, 2016), ECF No. 48 [hereinafter Stamper Order]; Michaud, 2016 WL 337263, at *4–5.

97   See Carlson R&R, supra note 93, at 26 ("This Court is not aware of any case where a court has permitted the actual identification of the place to be searched to depend upon the occurrence of an anticipated event that has not yet occurred."); see also Grubbs, 547 U.S. at 95–96 ("[W]hen an anticipatory warrant is issued, the fact that the contraband is not presently located at the place described in the warrant is immaterial, so long as there is probable cause to believe that it will be there when the search warrant is executed." (emphasis added) (internal citation omitted)).

98   See, e.g., Knowles, 2016 WL 6952109, at *4.

99   Id. at *12 (citing United States v. Karo, 468 U.S. 705, 718 (1984)). This rationale may also be used to argue that disclosure of the NIT's source code is necessary to determine whether or not the NIT warrant satisfies the Fourth Amendment.

100   Hammond, 2016 WL 7157762, at *3.This description is itself somewhat misleading as it suggests that the searches would be carried out in the Eastern District of Virginia (i.e., where the server was located). As discussed in detail below, the searches in fact occurred on the target computers.

101   See id. at *3.

102   Id. at *3.

103   Carlson R&R, supra note 93, at 24–26.

104   In re Warrant, 958 F. Supp. 2d at 759.

105   United States v. Weber, 923 F.2d 1338, 1342 (9th Cir. 1990) (citation omitted).

106   California v. Acevedo, 500 U.S. 565, 580 (1991); see also Matish, 193 F. Supp. 3d at 608; Darby, 190 F. Supp. 3d at 533; Michaud, 2016 WL 337263, at *5.

107   Marshall v. Barlow's Inc., 436 U.S. 307, 323 (1978).

108   Matish, 193 F. Supp. 3d at 607–09.

109   Darby, 190 F. Supp. 3d at 533.

110   Levin, 186 F. Supp. 3d at 44, 44 n.29; see also Carlson R&R, supra note 93, at 6–7.

111   In re Warrant, 958 F. Supp. 2d at 759.

112   Id. at 755–56.

113   Id. at 760 (citing United States v. Cuevas-Sanchez, 821 F.2d 248, 252 (5th Cir. 1987).

114   Id at 759–60.

115   28 U.S.C. § 636(a)(1).

116   Fed. R. Crim. P. 41(b) (emphasis added).

117   Fed. R. Crim. P. 41(b)(6) (emphasis added).

118   For example, Hammond, a Playpen case, was decided on December 8, 2016—a week after the
        new rule went into effect—but applied the old version given that the relevant warrant was issued
        before December 1, 2016. See also Dzwonczyk, 2016 WL 7428390, at *7–8 (decided December
        23, 2016).

119   Five courts have ruled that the magistrate who issued the Playpen NIT warrant lacked
        jurisdiction to do so, and that suppression of evidence is therefore required. Carlson R&R, supra
        note 93, at 11–22; Croghan, 2016 WL 4992105, at *8; Workman, 2016 WL 5791209, at *10;
        Arterbury R&R, supra note 72, at 27–28; Levin, 186 F. Supp. 3d at 44.

        Another twenty-six decisions considering the Playpen NIT warrant have ruled that, although the
        warrant was not properly issued pursuant to Rule 41, suppression is unwarranted. United States
        v. Pawlak, No. 3:16-CR-306-D(1), 2017 WL 661371, at *7 (N.D. Tex. Feb. 17, 2017); United States
        v. Perdue, No. 3:16-CR-305-D(1), 2017 WL 661378, at *5 (N.D. Tex. Feb. 17, 2017); Kahler, 2017
        WL 586707, at *6; Deichert, 2017 WL 398370, at *10; Memorandum and Order, United States v.
        Tran, No. 1:16-cr-10010-PBS (D. Mass. Dec. 23, 2016) [hereinafter Tran Order], ECF 71 No. 71;
        Dzwonczyk, 2016 WL 7428390, at *14; United States v. Vortman, No. 16-cr-00210-TEH-1, 2016
        WL 7324987, at *13 (N.D. Cal. Dec. 16, 2016); Owens, 2016 WL 7053195, at *8; Order on
        Defendants' Motion to Dismiss Indictment, Defendants' Motion to Suppress Evidence,
        Defendants' Motion to Exclude Evidence, and Third Order on Defendants' Motion to Compel
        Discovery at 16, United States v. Tippens, 3:16-cr-05110-RJB (W.D. Wash. Nov. 30, 216), ECF
        No. 106 [hereinafter Tippens Order]; Hammond, 2016 WL 7157762, at *5; United States v.
        Duncan, No. 3:15-cr-00414-JO, 2016 WL 7131475, at *3 (D. Or. Dec. 6, 2016); United States v.
        Stepus, No. 15-30028-MGM, 2016 WL 6518427, at *2 (D. Mass. Oct. 28, 2016); Memorandum
        of Opinion and Order at 11–13, United States v. Libbey-Tipton, No. 1:16-cr-00236-PAG (N.D.
        Oh. Oct. 19, 2016), ECF No. 19 [hereinafter Libbey-Tipton Order]; Scarbrough, 2016 WL
        5900152, at *1–2; United States v. Allain, -- F. Supp. ---, 2016 WL 5660452, at *11–12 (D. Mass.
        Sept. 29, 2016); Anzalone I, 2016 WL 5339723, at *11; Broy, 2016 WL 5172853, at *9; Ammons,
        2016 WL 4926438, at *8–10; Knowles, 2016 WL 6952109, at *10–18; Torres, 2016 WL 4821223,
        at *7; Henderson, 2016 WL 4549108, at *5–6; Adams, 2016 WL 4212079, at *8; Rivera Order,
        supra note 79, at 16–23; Werdene, 188 F. Supp. 3d at 452–53; Stamper Order, supra note 96, at
        21-23; Michaud, 2016 WL 337263, at *7.

        Finally, twelve decisions have ruled that the Playpen NIT warrant was properly issued under
        Rule 41 because it was authorized as a tracking device pursuant to Rule 41(b)(4). These courts
        have denied motions to suppress on this basis. See United States v. Austin, No. 3:16-CR-00068,
        2017 WL 496374, at *4 (M.D. Tenn. Feb. 2, 2017); United States v. Jones, No. 3:16-CR-026,
        2017 WL 511883, at *4 (S.D. Ohio Feb. 2, 2017); United States v. Sullivan, No. 1:16-CR-270,
        2017 WL 201332, at *6 (N.D. Ohio Jan. 18, 2017); McLamb Order, supra note 57, at 18; United
        States v. Lough, -- F. Supp. 3d ---, 2016 WL 6834003, at *5 (N.D.W. Va. Nov. 18, 2016); United
        States v. Johnson, No. 15-00340-01-CR-W-GAF, 2016 WL 6136586, at *6–7 (W.D. Mo. Oct. 20,

2016); Opinion and Order Denying Sealed Motion at 15, United States v. Smith, 4:15-cr-00467 (S.D. Tex. Sept. 28, 2016), ECF No. 41 [hereinafter Smith Order]; United States v. Jean, -- F. Supp. 3d ---, 2016 WL 4771096, at *16–17 (W.D. Ark. Sept. 13, 2016); Eure, 2016 WL 4059663 at *4 (incorporating Darby, authored by same judge); Matish, 193 F. Supp. 3d at 613; Darby, 190 F. Supp. 3d at 536–38; Epich, 2016 WL 953269, at *2. See also United States v. Kienast, No. 16-CR-103, 2016 WL 6683481, at *4 (E.D. Wis. Nov. 14, 2016) (would be reasonable to find that the warrant was valid under Rule 41(b)(4) and suppression is not warranted regardless); Laurita, 2016 WL 4179365, at *6 (same for Torpedo operation).

120   In re Warrant, 958 F. Supp. 2d at 757. On at least one occasion, the government argued that the search in question occurred on the servers hosting sites visited by the suspect's computer, but this argument was unsuccessful because, as the court explained, it is "not the server itself from which the relevant information [i]s sought" in a NIT case, but rather the suspect's computer. See Levin, 186 F. Supp. 3d at 33.

121   Levin, 186 F. Supp. 3d at 33–34. It should also be noted that at least one judge has questioned whether a defendant can challenge a NIT warrant in a watering hole case when his computer just so happened to be located in the district from which the warrant issued. See Matish, 193 F. Supp. 3d at 613 (finding no violation but then noting that, in any event, "as far as this case is concerned, all relevant events occurred in Virginia [where the warrant issued]"). Other Playpen cases arising in the district from which the Playpen NIT warrant was issued found no Rule 41(b) violation on other grounds, see Eure, 2016 WL 4059663, at *4; Darby, 190 F. Supp. 3d at 536–37, without even mentioning the special issue identified in Matish. Ultimately, moreover, the fact that a watering hole warrant requires a magistrate judge to approve searches that could occur anywhere in the world renders the warrant "void ab initio," as several courts have put it, Workman, 2016 WL 5791209, at *8; Levin, 186 F. Supp. 3d at 35, which likely means that a defendant whose computer was in the district from which the warrant issued can still raise a Rule 41(b) challenge.

122   Matish, 193 F. Supp. 3d at 612; see also McLamb Order, supra note 57, at 17–18; Smith Order, supra note 119, at 15; Jean, 2016 WL 4771096, *15; Darby, 190 F. Supp. 3d at 536 ("[u]sers of Playpen digitally touched down in the Eastern District of Virginia when they logged into the site" and installation of the tracking device therefore occurred within the district).

123   Hammond, 2016 WL 7157762, at *4.

124   Adams, 2016 WL 4212079, at *6; see also Dzwonczyk, 2016 WL 7428390, at *7; Libbey-Tipton Order, supra note 119, at 7–8; Levin, 186 F. Supp. 3d at 34; Michaud, 2016 WL 337263, at *6; see also Kahler, 2017 WL 586707, at *6 (fitting the NIT into the (b)(4) exemption would require "torturing the language" of the rule).

125   See Levin, 186 F. Supp. 3d at 34 (rejecting this claim); In re Warrant, 958 F. Supp. 2d at 757 (same).

126   Subsection (b)(3) is not, however, entirely irrelevant in non-terrorism cases. One court in a case involving the Playpen NIT warrant reasoned, for instance, that because the drafters expressly lifted all territorial limits for investigations involving terrorism in subsection (b)(3), they plainly "knew how to avoid the territorial limit on issuance of warrants when they wished to do so." Arterbury R&R, supra note 72, at 17. This expressio unius argument is a powerful one for warrants issued before December 1, 2016, and can be used to respond to the government's repeated urging of a "flexible application of the Rule" that would authorize extra-district searches. Werdene, 188 F. Supp. 3d at 441.

127   Workman, 2016 WL 5791209, at *4.

128   Arterbury R&R, supra note 72, at 17 n.7.

129   Torres, 2016 WL 4821223, at *6; see also Dzwonczyk, 2016 WL 7428390, at *8; Libbey-Tipton Order, supra note 119, at 8.

130   Acevedo-Lemus, 2016 WL 4208436, at *8.

131   Darby, 190 F. Supp. 3d at 536.

132   See, e.g., Levin, 186 F. Supp. 3d at 40 (not questioning this proposition).

133   Cf. Eure, 2016 WL 4059663, at *8 (culpability of the FBI agents "is reduced because of the need to obtain the warrant quickly.").

134   See, e.g., Darby, 190 F. Supp. 3d at 538 (finding suppression unwarranted even if the NIT warrant was void in part because "the officers in charge of this investigation are not at all culpable" and "[t]he FBI should be applauded for its actions in this case.").

135   Carlson R&R, supra note 93, at 11–22; Croghan, 2016 WL 4992105, at *8; Workman, 2016 WL 5791209, at *10; Arterbury R&R, supra note 72, at 27; Levin, 186 F. Supp. 3d at 42.

136   Carlson R&R, supra note 93, at 30.

137   Scarbrough, 2016 WL 5900152, at *1; Broy, 2016 WL 5172853, at *9; Ammons, 2016 WL 4926438, at *9. But see Croghan, 2016 WL 4992105, at *6 (NIT deployment constituted warrantless search and good-faith exception does not apply because warrant was void ab initio). In re Warrant finds constitutional defects in a NIT warrant, but did not involve a suppression motion. See In re Warrant, 958 F. Supp. 2d at 755 (denying application for search warrant). The Brooks court has not yet determined whether the NIT violated the Fourth Amendment.

138   Owens, 2016 WL 7053195, at *8.

139   See, e.g., Eure, 2016 WL 4059663, at *8; Matish, 193 F. Supp. 3d at 622–23; Darby, 190 F. Supp. 3d at 538–39; Werdene, 188 F. Supp. 3d at 452–53; Reibert, 2015 WL 366716, at *3.

140   United States v. Leon, 468 U.S. 897 (1984).

141   Reibert, 2015 WL 366716, at *3 (quoting United States v. Grant, 490 F.3d 627, 632 (8th Cir. 2007)). In the NIT warrant context, numerous courts have found that the magistrate judge who issued the warrant, rather than the law enforcement agents who sought it, was at fault and have accordingly refused to suppress the evidence obtained through the NIT because "[t]he FBI agents can hardly be faulted for failing 'to understand the intricacies of the jurisdiction of federal magistrates.'" Ammons, 2016 WL 4926438, at *9 (quoting Darby, 190 F. Supp. 3d at 538).

142   See Herring v. United States, 555 U.S. 135, 147–48 (2009); Arizona v. Evans, 514 U.S. 1, 14–16 (1995).

143   See Levin, 186 F. Supp. 3d at 40 (citing Herring v. United States, 555 U.S. 135, 142 (2009)).

144   Owens, 2016 WL 7053195, at *8; Scarbrough, 2016 WL 5900152, at *1; Broy, 2016 WL 5172853, at *9 ("[L]aw enforcement exhibited laudable conduct in this case."); Ammons, 2016 WL 4926438, at *9; but see Carlson R&R, supra note 93, at 19–22, 28–29.

145   Levin, 186 F. Supp. 3d at 41. Levin relied on the holding in United States v. Scott, 260 F.3d 512 (6th Cir. 2001), and dicta from several state-court cases for the proposition that exclusion is warranted under such circumstances. 186 F. Supp. 3d at 40 & n.17. Levin also correctly noted that the holding in Scott was repudiated by the Sixth Circuit in light of subsequent developments in the Supreme Court's exclusionary rule jurisprudence. Id. at 40 (citing United States v. Master, 614 F.3d 236, 239 (6th Cir. 2010)). While the Supreme Court's later cases indeed frame exclusion as the exception rather than the rule, the Supreme Court has never directly addressed the question of whether Leon applies when a warrant was issued in excess of a magistrate judge's jurisdiction, and it is fair to characterize this as an open question.

146   Levin, 186 F. Supp. 3d at 41 (citing United States v. Curzi, 867 F.2d 36 (1st Cir. 1989)).

147   Carlson R&R, supra note 93, at 15–16; Croghan, 2016 WL 4992105, at *6; Workman, 2016 WL 5791209, at *8; Arterbury R&R, supra note 72, at 26. But see Ammons, 2016 WL 4926438, at *8 (holding that good-faith exception is not foreclosed where warrant is void ab initio).

148   Herring, 555 U.S. at 141; see also Werdene, 188 F. Supp. 3d at 451–52 (heavily emphasizing the utilitarian calculus in finding suppression unwarranted).

149   Acevedo-Lemus, 2016 WL 4208436, at *8 ("The severe penalty of suppression should not be levied against the government (and society generally) merely because the government had the good sense to seek an amendment to Rule 41."); see also Werdene, 188 F. Supp. 3d at 451–52 (same).

150   Because any Fourth Amendment defects in NIT warrants are less obvious than the Rule 41(b) defects (as indicated by the analysis above and by the fact that more courts have found Rule 41(b) violations than Fourth Amendment violations), the balancing test is even less likely to favor defendants when applied to constitutional deficiencies that may be found in future cases.

151   See Werdene, 188 F. Supp. 3d at 442 (collecting cases).

152   See e.g., United States v. Hornick, 815 F.2d 1156, 1158 (7th Cir. 1987) (Easterbrook, J.) ("In light of Leon, it is difficult to anticipate any violation of Rule 41, short of a defect that also offends the Warrant Clause of the fourth amendment, that would call for suppression. Many remedies may be appropriate for deliberate violations of the rules, but freedom for the offender is not among them."); Acevedo-Lemus, 2016 WL 4208436, at *7; Matish, 193 F. Supp. 3d at 621–22. In the Eighth Circuit, recklessness suffices. See United States v. Spencer, 439 F.3d 905, 913 (8th Cir. 2006).

153   Carlson R&R, supra note 93, at 11–14, 19; Croghan, 2016 WL 4992105, at *6; Workman, 2016 WL 5791209, at *8; Arterbury R&R, supra note 72, at 26; Levin, 186 F. Supp. 3d at 36.

154   Carlson R&R, supra note 93, at 15–16; Workman, 2016 WL 5791209, at *8; Arterbury R&R, supra note 72, at 25–26; Levin, 186 F. Supp. 3d at 35 (citing United States v. Krueger, 809 F.3d 1109, 1115 n.7 (10th Cir. 2015)).

155   There is at least one federal appellate case that finds suppression was warranted for a "substantive" Rule 41(b) violation without finding that any of the defendant's Fourth Amendment rights were violated. See United States v. Glover, 736 F.3d 509, 515 (D.C. Cir. 2013). This case does not explicitly grapple with the question of whether there can be substantive Rule 41 violations that are not of constitutional magnitude, but simply assumes that to be the case. It should be cited, along with Levin (which relies on it), by defendants in NIT warrant cases where the availability of suppression for violation of Rule 41 is at issue.

156   Carlson R&R, supra note 93, at 15–16; Croghan, 2016 WL 4992105, at *6; see also Broy, 2016 WL 5172853, at *8.

157   Ammons, 2016 WL 4926438, at *6–7, 9.

158   Michaud, 2016 WL 337263, at *6 (alteration and citation omitted).

159   Adams, 2016 WL 4212079, at *7; see also Levin, 186 F. Supp. 3d at 37–38; Orin Kerr, Government 'hacking' and the Playpen search warrant, Washington Post, Sept. 27, 2016, https://www.washingtonpost.com/news/volokhconspiracy/wp/2016/09/27/government-hacking-and-the-playpen-search-warrant/?utm_term=.6603f6da28a3 (quoting United States v. Krueger, 809 F.3d 1109, 1114 (10th Cir. 2015)).

160   This problem would technically be surmountable if the government applied for NIT warrants in all 94 federal judicial districts. See Acevedo-Lemus, 2016 WL 4208436, at *7 (noting "burden and expense of such an undertaking"). That prospect is probably sufficiently remote, however, for a court to consider the defect essentially incurable. See Werdene, 188 F. Supp. 3d at 441–42 (emphasizing that this approach would be nearly impossible). At the same time, some courts have found no prejudice based on the assumption that a district judge could have issued the

warrant notwithstanding Rule 41(b)'s territorial limitations on magistrate judges. See Hammond, 2016 WL 7157762, at *5.

161   See Levin, 186 F. Supp. 3d at 38 (collecting examples of non-prejudicial defects). See also Pierce, 2014 WL 5173035, at *5.

162   See Adams, 2016 WL 4212079, at *8 (finding prejudice but denying suppression under good-faith exception); Arterbury R&R, supra note 72, at 19–23; Levin, 186 F. Supp. 3d at 37–38. But see Jean, 2016 WL 4771096, at *18 (finding no prejudice because a district judge could have authorized the warrant); Acevedo-Lemus, 2016 WL 4208436, at *7 (finding no prejudice because FBI could have acquired warrant in each district).

163   See, e.g., Michaud, 2016 WL 337263, at *7.

164   See Werdene, 188 F. Supp. 3d at 446–47 (citing United States v. Hall, 505 F.2d 961, 964 (3d Cir. 1974)); see also United States v. Searp, 586 F.2d 1117, 1125 (6th Cir. 1978) (describing the Third Circuit's test as "more restrictive").

165   See Hall, 505 F.2d at 964.

166   Werdene, 188 F. Supp. 3d at 451–52.

167   Matish, 193 F. Supp. 3d at 622 (quoting United States v. Simons, 206 F.3d 392, 403 (4th Cir. 2000)).

168   See Acevedo-Lemus, 2016 WL 4208436, at *8 (rejecting argument that proposed Rule 41 amendment shows government's bad faith); see also Hammond, 2016 WL 7157762, at *5; Knowles, 2016 WL 6952109, at *14.

169   Werdene, 188 F. Supp. 3d at 451–52.

170   Carlson R&R, supra note 93, at 29–30.

171   Hammond, 2016 WL 7157762, at *5–6; see also Perdue, 2017 WL 661378, at *5; Pawlak, 2017 WL 661378, at *7; United States v. Kim, No. 16-CR-191 (PKC), 2017 WL 394498 (E.D.N.Y. Jan. 27, 2017); Tran Order, supra note 119; United States v. Vortman, No. 16-CR-00210-TEH-1, 2016 WL 7324987, at *4 (N.D. Cal. Dec. 16, 2016); Tippens Order, supra note 119, at 10; United States v. Anzalone, No. 15-10347-PBS, 2016 WL 6476939, at *4 (D. Mass. Oct. 28, 2016) [hereinafter Anzalone II]; Allain, 2016 WL 5660452, at *13; Minute Entry, United States v. Michaud, No. 3:15-cr-05351-RJB (W.D. Wash. Jan. 22, 2016), ECF No. 135 (oral order denying motion to dismiss indictment); see also Order Denying Defendant's Motion to Dismiss for Outrageous Government Conduct at 2–3, United States v. Chase, 5:15-cr-00015-RLV-DCK-1 (W.D.N.C. Sept. 9, 2016), ECF No. 85.

172   See United States v. Bogart, 783 F.2d 1428, 1436 (9th Cir. 1986), vacated in part on other grounds, United States v. Wingender, 790 F.2d 802 (9th Cir. 1986).

173   See United States v. Archer, 486 F.2d 670, 677 (2d Cir. 1973).

174   See, e.g., United States v. Twigg, 588 F.2d 373, 379–81 (3d Cir. 1978) (finding dismissal warranted where government had provided so much direction and assistance to defendants in creating a drug laboratory that it had almost single-handedly fomented the entire crime).

175   Bogart, 783 F.2d at 1438.

176   Archer, 486 F.2d at 676–77.

177   Paroline v. United States, 134 S. Ct. 1710, 1726 (2014) (explaining the effect of viewing child pornography on the victims depicted).

178   United States v. Chin, 934 F.2d 393, 399 (2d Cir. 1991).

179   Tippens Order, supra note 119, at 8.

180   Id.; But see Tran Order, supra note 119, at 11–12 (rejecting this argument).

181   Tippens Order, supra note 119, at 8.

182   See United States v. Black, 733 F.3d 294, 302–03 (9th Cir. 2013) (noting that there is no bright line test to determine whether the government acted outrageously, but outlining the following factors for consideration: (1) known criminal characteristics of the defendants; (2) individualized suspicion of the defendants; (3) the government's role in creating the crime; (4) the government's encouragement to commit the offense; (5) the nature of the government's participation in the offense; and (6) the balance between the nature of the crime and the necessity of the conduct).

183   See, e.g., United States v. Owens, No. 16-CR-38-JPS, 2016 WL 7079617, at *5 (E.D. Wis. Dec. 5, 2016).

184   See, e.g., Vortman, 2016 WL 7324987, at *4; Allain, No. 15-CR-10251, 2016 WL 5660452, at *13.

185   Anzalone II, supra note 171, at *4.

186   Id. ("It is troubling that an agent stated that the Producer's Pen would be returning in the future because that section might have encouraged members to produce and share new child pornography (although there is no evidence it did so).").

187   Hammond, 2016 WL 7157762, at *5 (quoting government press release); see also The National Strategy for Child Exploitation and Prevention and Interdiction: A Report to Congress, U.S. Dep't of Justice (Aug. 2010), https://www.justice.gov/psc/docs/natstrategyreport.pdf; Victims of Child Pornography, U.S. Dep't of Justice, https://www.justice.gov/criminal-ceos/child-pornography (last visited Jan. 9, 2017) ("Once an image is on the Internet, it is irretrievable and can continue to circulate forever.").

188   Exhibit B - NIT Warrant Application ¶ 19, United States v. Matish, 4:16-cr-16 (E.D. Va. Mar. 17, 2016), ECF No. 18-2.

189   See, e.g., Anzalone II, supra note 171, at *4. But the Anzalone court suggested that the seeming increase in users after the FBI took control of the website was caused by fewer users logging in during the early stages of the website, and was in line with more recent trends.

190   Id. at *2.

191   Workman, 2016 WL 5791209, at *10.

APPENDIX A: GLOSSARY

Activating Computer: an individual computer that "triggers" malware by visiting a certain website or file download.

CIPAV: Computer and Internet Protocol Address Identifier. The term that the Federal Bureau of Investigation (FBI) used in documents revealed via a 2007 FOIA request to refer to a technology that, when installed on a user's computer, allows the FBI to collection identifying information such as an IP or MAC address. (https://www.eff.org/deeplinks/2011/04/new-fbi-documents-show-depth-government). See "Network Investigative Technique."

Dark Web: all websites that hide their IP addresses. These sites, often called hidden or onion services, cannot be found using typical search engines like Google. Users may only access the Dark Web via software known as Tor. Typically, but not always, users must know the exact URL of a Dark Website in order to visit it.

DarkNet: see "Dark Web."

Encryption: the conversion of electronic data into another form, called ciphertext, which masks the true content unless and until a decryption tool, called a "key," is used to reveal it. The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted via the internet or other computer networks. (http://searchsecurity.techtarget.com/definition/encryption)

Environment Variables: term used in affidavit and warrant applications to encompass operating system type and version, browser type and version, language the browser is using, and more.

Internet Service Provider: a company that provides customers with internet access.

IP Address: numeric address used to direct information over the internet, and which can be used to identify computers or other devices accessing the internet.

Tor: originally stood for The Onion Router. Software that allows its users to connect to the internet via a series of what it calls "virtual tunnels." Essentially, Tor enlists a network of volunteer servers through which it routes a user's internet activity. Functionally, this bounces the user's IP address from server to server, changing it and stripping the former IP address when the connection is routed through another "node." This preserves internet anonymity.

Tor Entry Node: the Tor relay node through which a Tor user first connects to the Tor network. The entry node receives the Tor user's website request, strips the request of identifying information and passes it on to the next relay node. Note that an entry node can view a Tor user's real IP address, although a user may employ techniques such as a "Virtual Private Network" (VPN) to hide their real IP address from the Tor entry node.

Tor Relay Node: a computer or server acting as a node in the Tor network that relays the Tor user's website request to the next node. This term encompasses the "Tor Entry Node."

Malware: a program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, operating system, or of otherwise annoying or disrupting the victim. (NIST SP 800-83 Rev. 1)

Network Investigative Technique: a broad term employed by the Federal Bureau of Investigation (FBI) and other law enforcement entities to refer to an investigative technique that involves "hacking" or remotely access a computer to install malicious software without the user's consent or permission to control the computer and often to collect information. (https://www.justsecurity.org/15018/justice-department-proposal-massive-expand-fbi-extraterritorial-surveillance/)

Watering Hole Attack: a security exploit in which the attacker seeks to compromise a specific group of end users by infecting websites that members of the group are known to visit. The goal is to infect a targeted user's computer and gain access to the network at the target's place of employment. (searchsecurity.techtarget.com/definition/watering hole-attack)

Network Level Message: an exchange of technical information between two computers.

MAC Address: a numeric address that uniquely identifies the network interface card in a computer, often used by the Federal Bureau of Investigation (FBI) or other law enforcement entities to associate online behavior with a specific piece of hardware.

Virtual Private Network: an encrypted network, built on top of existing physical networks, that provides a secure communications tunnel for data and other information transmitted between networks. A VPN is one way that a user can hide their IP address from the Tor entry node or from law enforcement surveillance techniques.

APPENDIX B: TABLE OF ORDERS ON MOTIONS TO SUPPRESS

Case	Date	Court	Case No.	Type	Search?	Fourth Am. violation?	Rule 41 violation?	Suppression?
In re Warrant to Search a Target Comput. at Premises Unknown	4/22/13	S.D. Tex.	958 F. Supp. 2d 753	Bank fraud/ identity theft	Yes.	Yes. Warrant affidavit lacks particularity.	Yes.	N/A: Warrant application denied.
U.S. v. Pierce	10/14/14	D. Neb.	2014 WL 5173035	Torpedo	Not reached.	No.	No (notice provision only).	No. No showing of prejudice or reckless disregard.
U.S. v. Reibert	1/27/15	D. Neb.	2015 WL 366716	Torpedo	Not reached.	No.	Not raised.	No. Good-faith exception applies.
U.S. v. Cottom	12/22/15	D. Neb.	2015 WL 9308226	Torpedo	Not reached.	No.	Not discussed.	No.
U.S. v. Michaud	1/28/16	W.D. Wash.	2016 WL 337263	Playpen	Not reached.	No, even if nets many people.	Yes (technical).	No. Good-faith exception applies. No showing of prejudice or deliberate disregard.
U.S. v. Stamper	2/19/16	S.D. Ohio	1:15-cr-109	Playpen	Not reached.	No.	Yes (technical).	No. Good-faith exception applies. No showing of prejudice or deliberate disregard.
U.S. v. Epich	3/14/16	E.D. Wis.	2016 WL 953269	Playpen	Not reached.	No.	No.	No.
U.S. v. Levin	5/5/16	D. Mass.	186 F. Supp. 3d 26	Playpen	Assumes yes.	Not reached.	Yes (substantive).	Yes. Defendant prejudiced, and good-faith exception inapplicable.
U.S. v. Arterbury	4/25/16	N.D. Okla.	15-CR-182-JHP	Playpen	Not reached.	Not reached.	Yes (substantive).	Yes. Good-faith exception cannot apply. Exigent circumstances exception does not apply.
U.S. v. Werdene	5/18/16	E.D. Pa.	188 F. Supp. 3d 431	Playpen	No.	No.	Yes (technical).	No. Did not offend fundamental fairness; no prejudice. Good-faith exception applies.

Case	Date	Court	Case No.	Type	Search?	Fourth Am. violation?	Rule 41 violation?	Suppression?
U.S. v. Darby	6/3/16	E.D. Va.	190 F. Supp. 3d 529	Playpen	Yes.	No, even if nets many people and describes homepage inaccurately.	No. Rule 41(b)(4).	No. Even if constitutional violation, not intentional.
U.S. v. Matish	6/23/16	E.D. Va.	193 F. Supp. 3d 585	Playpen	No.	No. No warrant required. Also, not anticipatory; inaccurate description immaterial and not intentional.	No. Rule 41(b)(4).	No. Even if needed warrant, good-faith exception applies. Even if rule violation, not constitutional, no prejudice, and no deliberate disregard.
U.S. v. Rivera	7/20/16	E.D. La.	2:15-cr-266-CJB-KWR	Playpen	Assumes yes (but also finds no in Rule 41 section).	No, sufficiently particular.	Yes (technical).	No. No prejudice, and good-faith exception applies.
U.S. v. Eure (same judge as *Darby*)	7/28/16	E.D. Va.	2016 WL 4059663	Playpen	Not reached.	No, not anticipatory and even if describes homepage inaccurately.	No. Relies on *Darby*.	No. Even if constitutional violation, diminished by need to obtain warrant quickly. Even if rule violation, not deliberate.
U.S. v. Laurita	8/5/16	D. Neb.	2016 WL 4179365	Torpedo	Not reached.	Not reached.	No. Rule 41(b)(4).	Not reached.
U.S. v. v. Acevedo-Lemus	8/8/16	C.D. Cal.	2016 WL 4208436	Playpen.	No.	No.	Not reached. Rule 41(b)(4) could apply.	No. Even if rule violation, not constitutional, no prejudice, not intentional. Good-faith exception applies.

Case	Date	Court	Case No.	Type	Search?	Fourth Am. violation?	Rule 41 violation?	Suppression?
U.S. v. Adams	8/10/16	M.D. Fla.	2016 WL 4212079	Playpen	Yes.	No.	Yes.	No. Rule violation was not intentional or deliberate. Defendant prejudiced, but good-faith exception applies.
U.S. v. Henderson	9/1/16	N.D. Cal.	2016 WL 4549108	Playpen	No.	No.	Yes (technical).	No. Defendant not prejudiced, FBI did not act with deliberate disregard, and warrant executed in good faith.
U.S. v. Workman	9/6/16	D. Co.	2016 WL 5791209	Playpen	Yes.	Not reached.	Yes (substantive).	Yes. Defendant prejudiced. Good-faith exception inapplicable where warrant is void *ab initio*.
U.S. v. Torres	9/9/16	W.D. Tex.	2016 WL 4821223	Playpen	Yes.	Not reached.	Yes (technical).	No. Rule violation not in bad faith.
U.S. v. Jean	9/13/16	W.D. Ark.	2016 WL 4771096	Playpen	Assumes yes but could find no.	No.	No. Rule 41(b)(4).	No. Even if rule violation, technical and defendant not prejudiced. Even if warrant were deficient, good-faith exception applies.
U.S. v. Knowles	9/14/16	D.S.C.	2016 WL 6952109	Playpen	Yes (privacy of contents seized).	No, particularity satisfied.	Yes (technical).	No. Not void *ab initio*. No prejudice. Good-faith and exigent circumstance exceptions apply.
U.S. v. Ammons	9/14/16	W.D. Ky.	2016 WL 4926438	Playpen	Yes.	Yes.	Yes (substantive).	No. Good-faith exception applies even though warrant void *ab initio*.
U.S. v. Croghan	9/19/16	S.D. Iowa	2016 WL 4992105	Playpen	Yes.	Not reached.	Yes (substantive).	Yes. Warrant was void *ab initio* and good-faith exception cannot apply. Defendant prejudiced.
U.S. v. Broy	9/21/16	C.D. Ill.	2016 WL 5172853	Playpen	Yes.	Yes (through Rule violation)	Yes (substantive).	No. Good-faith exception applies, and no prejudice.
U.S. v. Anzalone	9/22/16	D. Mass.	2016 WL 5339723	Playpen	Yes.	No, even if inaccurate description; triggering event occurred.	Yes.	No. Good-faith exception applies, and warrant not void *ab initio*.

Case	Date	Court	Case No.	Type	Search?	Fourth Am. violation?	Rule 41 violation?	Suppression?
U.S. v. Smith	9/28/16	S.D. Tex.	4:15-CR-00467	Playpen	Not reached.	No.	No. Rule 41(b)(4).	No. Even if violation, good-faith exception applies.
U.S. v. Allain	9/29/16	D. Mass	2016 WL 5660452	Playpen	Not reached.	No.	Yes (technical).	No. Good-faith exception applies.
U.S. v. Scarbrough	10/11/16	E.D. Tenn.	2016 WL 5900152	Playpen	Yes.	Yes.	Yes.	No. Good-faith exception applies.
U.S. v. Libbey-Tipton	10/19/16	N.D. Ohio	1:16 CR 236	Playpen	Not reached.	Not reached.	Yes (assumes substantive).	No. Good-faith exception applies.
U.S. v. Johnson	10/20/16	W.D. Mo.	2016 WL 6136586	Playpen	Assumes yes (but not for IP address).	No.	No. Rule 41(b)(4).	No. Even if violation, good-faith exception applies, and no prejudice.
U.S. v. Stepus	10/28/16	D. Mass.	2016 WL 6518427	Playpen	Not reached.	Not reached.	Yes (technical).	No. Good-faith exception applies.
U.S. v. Kienast	11/14/16	E.D. Wis.	2016 WL 6683481	Playpen	Not reached.	No.	Not reached.	No. Warrant may have been valid under Rule 41(b)(4) and good-faith exception applies regardless.
U.S. v. Lough	11/18/16	N.D. W.Va.	2016 WL 6834003	Playpen	No.	No.	No. Rule 41(b)(4).	No. Even if violation, good-faith exception applies, and no prejudice.
U.S. v. McLamb	11/28/16	E.D. Va.	2:16cr92	Playpen	Not reached.	No.	No. Rule 41(b)(4).	No.
U.S. v. Tippens	11/30/16	W.D. Wash.	16-Cr-5110RJB	Playpen	Not reached.	No.	Yes (technical).	No.
U.S. v. Owens	12/5/16	E.D. Wis.	2016 WL 7053195	Playpen	Yes.	Yes.	Yes.	No, in light of Seventh Circuit precedent.
U.S. v. Duncan	12/6/16	D. Or.	2016 WL 7131475	Playpen	Yes.	No.	Yes (technical).	No. Warrant not void *ab initio*. No prejudice and good-faith exception applies.
U.S. v. Hammond	12/8/16	N.D. Cal.	2016 WL 7157762	Playpen	Yes.	No, sufficient particularity.	Yes (technical).	No. No prejudice and no evidence of deliberate disregard.
U.S. v. Vortman	12/16/16	N.D. Cal	2016 WL 7324987	Playpen	Yes.	No.	Yes (technical).	No. Good-faith exception applies.

Case	Date	Court	Case No.	Type	Search?	Fourth Am. violation?	Rule 41 violation?	Suppression?
U.S. v. Brooks	12/22/16 (R&R)	W.D. N.Y.	2016 WL 7409852	Playpen	Requested additional briefing & evidentiary hearing.	Requested additional briefing & evidentiary hearing.	Not reached.	Not reached.
U.S. v. Dzwonczyk	12/23/16	D. Neb.	2016 WL 7428390	Playpen	Yes.	No.	Yes (technical).	No. No prejudice and good-faith exception applies.
U.S. v. Tran (same judge as *Anzalone*)	12/28/16	D. Mass.	16-10010-PBS	Playpen	Not reached.	No. Relies on *Anzalone*.	Yes.	No. Relies on *Anzalone*.
U.S. v. Sullivan	1/18/17	N.D. Ohio	2017 WL 201332	Playpen	Not reached.	No.	No. Rule 41(b)(4).	No.
U.S. v. Deichert	1/28/17	E.D.N. C.	2017 WL 398370	Playpen	Not reached.	No.	Yes (technical).	No.
U.S. v. Austin	2/2/17	M.D. Tenn.	2017 WL 496374	Playpen	Not reached.	Not reached.	No. Rule 41(b)(4).	No. Even if violation, no deterrence.
U.S. v. Jones	2/2/17	S.D. Ohio	2017 WL 511883	Playpen	Assumes yes.	Not reached.	No. Rule 41(b)(4).	No. Even if violation, good-faith exception applies.
U.S. v. Kahler	2/14/17	E.D. Mich.	2017 WL 586707	Playpen.	Yes (incl. IP address).	No.	Yes.	No.
U.S. v. Pawlak	2/17/17	N.D. Tex.	2017 WL 661371	Playpen	Assumes yes.	No.	Yes (technical).	No. Good-faith exception applies.
U.S. v. Perdue (same judge as *Pawlak*)	2/17/17	N.D. Tex.	2017 WL 661378	Playpen	Assumes yes.	No.	Yes (technical).	No. Good-faith exception applies.
U.S. v. Carlson	3/23/17 (R&R)	D. Minn.	16-317 (JRT/FLN)	Playpen	Yes.	Yes, lacked particularity.	Yes (substantive).	Yes. Warrant was void *ab initio* and good-faith exception cannot apply. Defendant prejudiced.

APPENDIX C: SAMPLE BRIEFS AND LETTERS TO COMPEL DISCOVERY

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 2:16cr92
	)	
██████████████	)	

_____

DEFENDANT'S MOTION TO COMPEL DISCOVERY

████████████, through counsel and pursuant to Federal Rule of Criminal Procedure 16(d), respectfully moves this Court for an order compelling discovery material to trial and the defense's pending motions to suppress, ECF Nos. 14 and 15.

*　　*　　*

The defense asks the Court to order the government to provide the source code or programming code for the exploit that the government used to gain access to ██████████'s computer as well as discovery on the unique identifier generator through which the government purports to link ████████ to particular activity on the Playpen website. Earlier today, the government provided undersigned counsel a letter in which the government invoked a "law enforcement privilege" and stated its intent not to provide this data, even under a protective order.

The defense is seeking a copy of the exploit and ID generator so that a computer forensics expert can independently determine the full extent of the vulnerability created by the government on ██████████'s computer when it deployed the NIT; 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. This forensic information is relevant to ████████'s First and Second Motions to Suppress. *See United*

1

States v. Cranson, 453 F.2d 123, 127 n.6 (4th Cir. 1971) ("The defendant has remedies to secure pre-trial information on identification procedures undertaken by the Government in advance of trial as a basis for a motion to suppress."); *United States v. Wilford*, 961 F. Supp. 2d 740, 756 (D. Md. 2013), *on reconsideration in part* (Nov. 27, 2013) (holding that "information material to the Motion to Suppress, although sought in connection with a pretrial proceeding, might alter the 'quantum of proof'" at trial and is therefore discoverable under Rule 16). The discovery is also relevant to assessing other potential pretrial issues that the lack of discovery has thus far prevented the defense from being able to adequately evaluate. Indeed, one of the FBI's lead investigators on the Playpen case has stated in a declaration that "[d]etermining whether the government exceeded the scope of the [NIT] warrant thus requires an analysis of the NIT instructions delivered to [the defendant's] computer." Decl. of FBI Special Agent Daniel Alfin in Support of Gov't. Mot. for Reconsideration, at ¶ 7, in *United States v. Michaud*, Crim. No. 15-5351, ECF No. 166-2 (W.D. Wash. Mar. 28, 2016).

The requested items are also material to preparing a defense at trial. For example, the defense needs access to the code for the unique identifier to see how the government was purportedly able to link the information it collected to a particular computer or to a particular deployment of the NIT. And the defense needs to investigate the chain of custody for data collected remotely by the NIT. The need for these two critical components—the unique ID generator and the exploit—are discussed in the declaration of Vlad Tsyrklevich, which is being filed in this case under seal because of its sealed status in *Michaud*. *See* Ex. A (SEALED), Tsyrklevich Decl. from *Michaud*. The Office of the Federal Public Defender for the Eastern District of Virginia is also representing the defendant in related cases before Judge Morgan, *United States v. Matish*, Crim. No. 4:16cr16 (E.D. Va. Apr. 6, 2016), and Judge Doumar, *United*

2

45

States v. Eure, No. 2:16cr43 and *United States v. Darby*, No. 2:16cr36.   Professor Matthew

Miller has been retained by this Office in *Matish*, *Darby*, and *Eure* and his declaration explaining

the materiality of the requested technical evidence is also attached here as well.   *See* Ex. C, Decl.

of Dr. Matthew Miller.   Dr. Christopher Soghoian has also been retained as a defense expert on

these issues and may be called to testify at a hearing.

Although all of the questions discussed above are material to ██████████'s trial

defense, to date, the government has provided no actual evidence on these issues.   The exploit

and unique ID generator hold the answers to these questions.   But the government is apparently

unwilling to produce them.   Instead, the government is willing to provide the conclusions that it

believes can be drawn from its technological evidence.   Here, the defense requests access to the

evidence upon which the government's proposed conclusions are based.

Due process demands that ██████████ be afforded the opportunity to verify that the

government's evidence actually supports its allegations.   The government's monopoly on the

forensic evidence will allow its expert to testify at trial about what the NIT did, how it collected

information, and how it allowed the government to verify what the user of ██████████'s

computer was doing and when.   By invoking the law enforcement privilege, the government

seeks to deny ██████████ access to the underlying data upon which the government's key

expert testimony against him will rest.

It is worth noting that, in connection with other NIT/Playpen cases, courts have ordered

the government to make this very evidence available to the defense for inspection and forensic

analysis.   *See* Order Granting Third Motion to Compel Discovery in *Michaud*, Crim. No. 15-

5351, ECF No. 161 (W.D. Wash. Feb. 17, 2016) (ordering government to provide full NIT

evidence, including the exploit, in Playpen case).   In its letter to undersigned counsel, the

government suggested that the NIT source code is not "material" under Rule 16. But even on that specific issue, other federal judges have disagreed. Analyzing the materiality of the NIT source code in a Playpen case, the *Michaud* court held:

> I am satisfied that the defense has shown materiality here to preparing the defense…. The government hacked into a whole lot of computers on the strength of a very questionable search warrant. … Much of the details of this information is lost on me, I am afraid, the technical parts of it, but it comes down to a simple thing. You say you caught me by the use of computer hacking, so how do you do it? How do you do it? A fair question.

Order, ECF No. 205, 2 in *United States v. Michaud*, Case No. 3:15cr5351 (W.D. Wash. May 18, 2016) (quoting ECF No. 162, 17-19) (attached as Exhibit D). In the same order, the *Michaud* court further explained,

> The defendant is not required to accept the government's assurances that reviewing the N.I.T. code will yield no helpful information. ***The government asserts that the N.I.T. code will not be helpful to the defense, but that information may well, in the hands of a defense lawyer with a fertile mind, be a treasure trove of exculpatory evidence.***

Id., at 4 (emphasis added). Thus, the *Michaud* court held that the full NIT source code is material under Rule 16 and may well constitute *Brady* material.

In other cases involving NITs, the Department of Justice has not invoked a "law enforcement privilege," but rather has volunteered to make the programming code available for inspection by the defense. S*ee, e.g.,* Ex. B, at 2 (Department of Justice notice and disclosure letter in *United States v. Cottom*, Crim Nos. 8:13-108, 8:15-239 (D. Neb. Dec. 22, 2015), summarizing government's disclosures about NIT "Flash application" used in that case, including "example programming code," and extending an offer for defense inspection of the "compiled code for the NIT" stored on government server).

The defense is prepared to enter into a protective order to address any legitimate confidentiality concerns the government may have about disclosing the exploit.   Still, the Government says that it will not produce it, asserting that it is "subject to law enforcement privilege." To the extent the government needs to protect the confidentiality of the exploit, confidentiality can be achieved through the entry of a protective order.

Rule 16 and fundamental notions of due process preclude the government from refusing to allow the defense to inspect the key forensic evidence at issue in this case.   Yet that is the government's position.   By invoking a law enforcement privilege, the government asks ▮▮ ▮▮▮▮▮▮ and the Court to accept without verification the government's representations about what their technology did and how it works—questions critical to the defense's pending motions and to trial.   Here, the government used a sophisticated surveillance tool and then put ▮▮ ▮▮▮▮▮▮'s liberty at stake by initiating a prosecution based on information it gained through that surveillance.   It cannot now, in fairness, claim that the means by which it obtained the evidence it plans to use against ▮▮▮▮▮▮ is subject to a privilege that trumps ▮▮▮▮▮▮'s right to due process.

<p style="text-align:center">*   *   *</p>

For the reasons stated above, ▮▮▮▮▮▮ respectfully requests that the Court issue an Order for disclosure of the records and information sought by the defense, subject to such conditions or protections that the Court deems appropriate to address any legitimate confidentiality interests on the part of the Government.

Respectfully submitted,

▮▮▮▮▮▮▮▮

By:_____/s/_____

5

48

Amanda C. Conner
VSB # 88317
Attorney for ███████████
Office of the Federal Public Defender
150 Boush Street, Suite 403
Norfolk, Virginia 23510
(757) 457-0816
(757) 457-0880 (telefax)
amanda_conner@fd.org

Andrew W. Grindrod
VSB # 83943
Assistant Federal Public Defender
Attorney for ███████████
Office of the Federal Public Defender
150 Boush Street, Suite 403
Norfolk, Virginia 23510
(757) 457-0800
(757) 457-0880 (telefax)
andrew_grindrod@fd.org

6

U.S. Department of Justice

Criminal Division

Child Exploitation and Obscenity Section

1400 New York Ave., NW
Suite 600
Washington, DC 20530
(202) 514-5780 FAX: (202) 514-1793

November 7, 2014

Dear Counsel:

Pursuant to Rule 16(a)(1)(G) of the Federal Rules of Criminal Procedure, the government hereby discloses that it intends to elicit testimony from Federal Bureau of Investigation ("FBI") Special Agent ("SA") Steven A. Smith, Jr. and FBI Supervisory Special Agent ("SSA") P. Michael Gordon, under Federal Rules of Evidence 702, 703, or 705. Pursuant to Rule 16(b)(1)(C) of the Federal Rules of Criminal Procedure, the government hereby requests from defendant disclosure of testimony he intends to use under Rule 702, 703 and/or 705 of the Federal Rules of Evidence as evidence at trial.

The CVs of SA Smith and SSA Gordon are attached. Their testimony will be based upon their respective knowledge, skills, training and experience in the areas of computer forensics, computer programming, computer networking and network management and analysis, computer forensic data acquisition and analysis, investigations in child exploitation cases, the Internet, and forensic analysis of digital media including computers, computer servers, and websites. They may also testify regarding the Internet, the forensic examination of computers and digital media, and how the Internet is used to trade child pornography. Specifically, they may testify about the following topics:

- The Onion Router ("Tor") anonymity network, including its origin, structure, function, configuration and software applications; the Tor browser bundle; other methods to access the Tor network, such as tor2web and onion.to; and investigative strategies to identify users of the Tor network. Please note that detailed information about the Tor network, its structure and function, is publicly available at the Tor project website, www.torproject.org.

- the structure, operation, monitoring and seizure of data from the websites your clients are charged with accessing. Such testimony may include a description of the structure, function, and content of the website, including the child pornography available (as further described in your client's Indictment, the search warrant affidavit authorizing the deployment of a Network Investigative Technique on the pertinent website, and the search warrant affidavit authorizing a search of your client's residence, all of which you have been provided through discovery); unique session identifiers that track a user's activity on the site; the particular web pages accessed by a user during one of those sessions; and particular child pornography images/videos accessed by a user during one of those sessions. Such testimony may include but not be limited to the operation of websites, computers and computer servers, and related technical terms/concepts including HTML, HTTP,

PHP, Flash, and Javascript. Please note that a working offline copy of each of those websites has been made available to you and/or an expert of your choosing for examination. Further, through discovery, you were provided reports documenting data obtained from those computer servers, including data pertinent to your client's actions on the site. In addition, as we have previously advised you, the computer server(s) that hosted the websites are, and remain, available for examination by you or your chosen expert.

- the "Network Investigative Technique" ("NIT") that was deployed on each website and the admission of evidence obtained through the use of that technology. Such testimony may include: technical concepts underlying the use of technology such as the NIT, including but not limited to Flash, TCP, proxy servers, IP addresses, web browsers, computer servers, and exploits; the programming and operation of websites and computer servers; and the programming, testing and deployment of computer code on websites and computer servers; the configuration and deployment of the particular NIT utilized on the websites your clients accessed; and pre-deployment testing performed regarding the particular NIT utilized on the websites your clients accessed.

You have previously been provided reports documenting data obtained via the use of the NIT, which includes IP address information, session identifier information, operating system and architecture type. We have also previously disclosed to you via e-mails dated September 4, 2014, and September 23, 2014, incorporated herein by reference, details regarding where the particular NIT code was obtained and how it operated. In particular, as described in my September 4, 2014, e-mail message, the technique utilized a Flash application that, when downloaded by a user and activated by their browser, made a direct TCP connection to a server that the FBI controlled. Depending on the operating system and version of the user's browser, the connection would bypass the browser's configured proxy server and reveal the user's true IP address. In addition, the NIT also sent the user's operating system name and architecture type. Please also see my September 4, 2014 e-mail for example programming code for the Flash application itself. Further, as noted above and in my September 4 and 23 e-mails, the computer servers that hosted the pertinent websites contain the compiled code for the NIT. Those servers have been, and remain, available for examination by an expert of your choice. The experts disclosed herein may testify based upon their knowledge, skills, training and experience, as to any matters disclosed therein.

In order to avoid any confusion regarding the operation of the NIT, I offer the following further description of its functionality, about which the experts disclosed herein may testify.

The NIT was a Flash application. Flash applications are commonly present on numerous Internet websites. The NIT did not consist of a virus or "malware."

The NIT took advantage of a potential vulnerability in the configuration of a user's computer. When a user accessed a page on one of the pertinent websites where the NIT had been deployed, the NIT computer code would be downloaded to a user's computer along with the images/text/content that made up that web page. If a user's web browser was not configured to block Flash applications, then the NIT, once downloaded by a user's computer, would cause the computer to send a communication (in other words, a request) to a government-controlled computer that revealed the computer's IP address, a session identifier, the computer's operating

system and architecture. If a user's web browser was configured to block Flash applications, then the NIT would not successfully cause the computer to send such a request. As of November of 2012, the up-to-date Tor browser bundle was configured to block such Flash applications. Accordingly, the NIT would not have revealed the IP address of such a user, or of a user who had manually configured his/her browser to connect to the Tor network and opted to block Flash applications. Because none of your clients were using the up-to-date Tor browser bundle to access the website in question, and none of your clients configured his computer to block Flash applications, the NIT successfully identified your client's IP address.

Special Agent Smith and Supervisory Special Agent Gordon may also testify based upon their knowledge, skills, training and experience in the area of computer forensics, computer forensic data acquisition and analysis, investigations in child exploitation cases, and the Internet, as to the following matters:

·   regarding the Internet, which is a collection of computers and computer networks which are connected to one another via high-speed data links and telephone lines for the purpose of communicating and sharing data and information;

·   that connections between Internet computers exist across state and international borders; and that the Internet is a means of interstate and international communication; indeed, information sent between two computers connected to the Internet frequently crosses state and international borders even when the two computers are located in the same state;

·   regarding modems, and how a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Electronic contact can be made to literally millions of computers around the world;

·   regarding Internet Service Providers. Individuals and businesses obtain access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using telephone or other telecommunications lines; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or businesses that have subscriber accounts with them. Those records often include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, and other information both in computer data and written record format;

·   regarding IP Addresses. An Internet Protocol address ("IP address") is a unique numeric address used by each computer on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be properly directed from its source to its destination. Most ISPs control a range of IP addresses;

·   that when a customer logs into the Internet using the service of an ISP, the computer used

by the customer is assigned an IP address by the ISP. The customer's computer retains that IP address for the duration of that session (i.e., until the user disconnects), and the IP address cannot be assigned to another user during that period;

· regarding four basic functions computers and the Internet serve in connection with child pornography: production, communication, distribution, and storage;

· regarding how individuals can use computers and the Internet to meet, communicate with each other, and share files, including but not limited to websites, chat rooms, message boards, email, instant messaging, news groups, social networking sites, peer-to-peer programs, ICQ;

· regarding how child pornographers can transfer non-digital photographs from a camera into a computer-readable format a scanner, and how digital cameras allow images to be transferred directly onto a computer. Digital cameras often embed information into digital pictures, known as metadata, that identifies the camera used to take the picture;

· regarding how a computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store hundreds of thousands of images and videos at very high resolution;

· regarding how digital images/videos can be stored on external storage media such as thumb drives, compact disks, external hard drives, mp-3 players, smart phones, and how digital images/videos can be easily transferred from one digital device to another;

· regarding dedicated online storage space, such as the "FTP," or "File Transfer Protocol" site, and how such a site allows Internet users to maintain a massive and secure private library of child pornography that is available for viewing or download only by a certain group of individuals, such as members of the PedoBook online bulletin board;

· regarding user-created message boards, and how they can be easily created with free or inexpensive software and commercial web hosting companies;

· regarding forensic hashing, which is the process of using a mathematical function, often called an algorithm, to generate a numerical identifier for data (such as a particular file). If the data is changed, even very slightly (such as the addition or deletion of a comma or a period), the identifier should change. A hash value can be thought of as a "digital fingerprint" for data;

· regarding the use of a "hash set" which contains the hash values of image and video files associated with known identified victims of child pornography to determine whether these files are stored within a digital device;

·   The process of obtaining and verifying an image of a computer media item, bit-stream copies, and Message-Digest algorithm 5 (MD5) hash values;

·   Specialized computer terms, including, but not limited to, terms mentioned in this notice and in his report, such as ".html," ".lnk" ".jpg," ".mpg," ".avi," "cookie file," and "file slack;"

·   Evidence of web browsing activity and e-mail communications, including, but not limited to, fragments of web pages accessed, cookie files, e-mail messages, and other Internet-based communications stored in locations including, but not limited to, the temporary Internet file folders, file slack, and unallocated space;

·   The operation, analysis and investigation of websites, bulletin boards, social networking platforms and other Internet technologies dedicated to the sexual exploitation of children;

·   Online undercover tactics and techniques pertinent to the investigation, identification and apprehension of suspects engaging in online sexual exploitation of children;

·   Methods, tactics and techniques of individuals who seek to exploit children online.

Please contact me, Assistant U.S. Attorney Michael Norris or Trial Attorney Sarah Chang or if you have any questions about any of the information provided.

Sincerely,

/s/ Keith Becker_____
Keith Becker
Trial Attorney
Child Exploitation and Obscenity Section
Criminal Division
United States Department of Justice

Enclosures

P. MICHAEL GORDON
801 International Drive
Linthicum Heights, MD 21090

PROFESSIONAL EXPERIENCE

United States Department of Justice
    Federal Bureau of Investigation- Special Agent   03/1999 - Present

New Orleans Field Office   07/1999 - 02/2007

Investigated federal white collar crime violations for
approximately two years. Investigated cyber crimes for
approximately six years to include cyber intrusions and served
on the regional Cyber Action Team.

Innocent Images National Initiative   08/2004 - 02/2007

Served as the National Initiative case agent for the New Orleans
Field Office Innocent Images investigation. Conducted 79
original method Peer to Peer file share investigation sessions.
Participated in the testing and development of the eP2P FBI
investigative tool.

FBI Assignments

Hazardous Material Response Team (HMRT)	10/1999 - 02/2007
Assistant Team Leader HMRT	06/2002 - 02/2007
Relief Supervisor	03/2005 - Present
Cyber Squad, New Orleans	03/2005 - 02/2007
Major Case Coordination Unit, FBIHQ	02/2007 – 03/2014
Violent Crimes Against Children Unit, FBIHQ	03/2014 - Present

FBI Innocent Images Unit / Major Case Coordination Unit   02/2007 – 03/2014

Assigned to investigate international and domestic
incidents of child exploitation and the use of file sharing net-
works in the distribution of child pornography. Lead investi-
gations focused on the identification, location, and arrest of
individuals and groups involved in the trade, distribution, and
production of child pornography and the sexual exploitation
of children via the Internet..

Operation Achilles   02/2007 - 02/2009

Served as the co-case agent investigating an international

enterprise focused on individuals who utilized newsgroups and sophisticated security practices such as multiple layers of encryption for messages and content and regular use of proxy IP addresses for the trade and distribution of child pornography. The case was the first conviction under Title 18, U.S.C. 2252A and resulted in seven life sentences for 14 indicted subjects. The case won the Criminal Division's Assistant Attorney General Award.

Operation Green Ocean   08/2010 - 12/2012

Served as the case agent investigating an international conspiracy involving 21 individuals utilizing Facebook to traffic child pornography images. Six U.S. targets were convicted and sentenced.

Foreign Bulletin Board   10/2011

Oversaw the review and triage of a foreign language bulletin board which consisted of over 177 thousand sub-forums, 119 thousand threads, and over 76 thousand active posters responsible for over 1.7 million posts, over 125 thousand attached image files, and over 1 million links to third-party hosting sites. Additional translation of posts, categorization of attached files, and geo-location of over 520 thousand unique IP addresses was necessary in order determine potential targets based on the volume of data.

FBI Violent Crimes Against Children Unit

Currently assigned as program coordinator for online child   03/2014 - Present
exploitation investigations and special projects

COMPUTER TRAINING

Basic Innocent Images Training	04/2003
Dallas Crimes Against Children Conference	08/2006
Image Scan Training	11/2006
Advanced Innocent Images Training	04/2007
A+ Certification	04/2009
Net+ Certification	12/2009
Cyber Special Agent Career Path Stage II Completed	10/2009
Cyber Special Agent Career Path Stage III Completed	12/2009
Cyber Special Agent Career Path Stage IV Completed	04/2011

INSTRUCTIONAL EXPERIENCE

IACLEA Southeast Region, New Orleans, LA	2005
ROCIC Conference, Greensboro, SC	2005
Enhanced Peer-to-Peer Training	03/2006
Lake Charles Local LE training, Baton Rouge, Louisiana	2006
FBI Basic Online Undercover Training (Innocent Images)	2007 - Present
Online Covert Employee Course	2008 - Present
National ICAC Conference, San Jose, CA	05/2007
-eP2P file share investigation techniques	
National ICAC Conference, Columbus, OH	05/2008
-eP2P file share investigation techniques	
ICAC Training Class, NCMEC, Alexandria, VA	2008
-eP2P file share investigation techniques	
Regional ICAC Conference, San Jose, CA	05/2009
-Operation Achilles (co-presenter)	

Overseas Instruction

International Training Assistance Unit, Poland	2004
-Basic Cyber Crime Overview and Techniques	
International Training Assistance Unit, United Arab Emirates	2005
-Basic Cyber Crime Overview and Techniques	
International Training Assistance Unit, Romania	2006
-Basic Cyber Crime Overview and Techniques	
Pacific Training Initiative, Thailand	2007
-Innocent Images Overview and Techniques	
Pacific Training Initiative, Philippines	2009
-Innocent Images Overview and Techniques	

COURTROOM TESTIMONY

United States v. Robert Myron Latham, DNV	2008
-Testified as the investigating undercover agent and to the methods, procedures and function of P2P file sharing	
United States v. Andrew Edward Flyer, DAZ	2008
-Testified as an expert in P2P investigative techniques	
United States v. William Ernest Fuller, DAZ	2008
-Testified as an expert in P2P investigative techniques	
United States v. James Freeman, et. al (Op. Achilles), NDFL	2009
-Testified on six occasions to identification of subjects and forensic review of the computer evidence	
United States v. David Chiaradio, DRI	2010
-Testified as an expert on the eP2P investigative tool	
United States v. Max Budziak, NDCA	2011
-Testified as an expert on the eP2P tool and file share	

investigations

State of Illinois v. Manuel Sanchez   2011
    -Testified as the investigating undercover agent and
    methods, procedures and function of P2P file sharing

United States v. Paul Stanley, DMD   2012
    -Testified as expert in P2P programs and investigations

United States v. James Driver, EDMI   2012
    -Testified as expert in P2P programs and investigations

United States v. Christopher Myers, DMD   2012
    -Testified as expert in P2P programs and investigations

United States v. Alan Clifton, DMD   2013
    -Testified as expert in P2P programs and investigations

United States v. Timothy Defoggi, DNE   2014
    -Testified as expert in online investigations, Internet /
    anonymous network basics, websites that facilitate the
    trafficking of child exploitation material, and methods/
    tactics/operations of trafficking child exploitation material
    via the Internet

United States v. Paul Wencewicz, et al, DMT   2014
    -Testified as expert regarding investigations related to
    online bulletin boards

EDUCATION

United States Naval Academy
    Bachelor of Arts, Physics   1993

MILITARY EXPERIENCE

United States Marine Corps   1993 - 1999
    The Basic School (TBS) and Basic Armor Officer Course   1993 - 1994
    Platoon Commander, 1st Tank Battalion, Bravo Company   1994 - 1996
    Executive Officer, HQ Service Company, 1st Tank Bn   1996 - 1997
    Project Officer, Marine Corps Warfighting Lab   1997 - 1999

Steven A. Smith Jr.
2635 Century Parkway NE
Atlanta, GA 30345

PROFESSIONAL EXPERIENCE

United States Department of Justice

    Federal Bureau of Investigation- Special Agent   11/2007 – Present

Cleveland Field Office, Toledo Resident Agency   11/2007 – 10/2011

Investigated federal crimes involving the possession, receipt, distribution and production of child pornography and cyber crimes involving phishing/vishing attacks, VoIP intrusions, website intrusions, ACH fraud, botnets, credit card fraud, and Distributed Denial of Service (DDos) attacks.

FBI Violent Crimes Against Children, Major Case
Coordination Unit Headquarters   10/2011 – 10/2014

Investigated international and domestic incidents of child exploitation and the use of bulletin board systems in the distribution of child pornography. Involved in the review and triage of over 15 bulletin boards of varying types. Lead investigations focused on the identification, location, and arrest of individuals and groups involved in the trade, distribution, and production of child pornography and the sexual exploitation of children via the Internet.

Foreign Bulletin Board   12/2011 – 02/2012

Developed the technique and process for the review and triage of a foreign language bulletin board which consisted of over 177 thousand sub-forums, 119 thousand threads, and over 76 thousand active posters responsible for over 1.7 million posts, over 125 thousand attached image files, and over 1 million links to third-party hosting sites. In addition, translation of posts, categorization of attached files, and geo-location of over 520 thousand unique IP addresses was necessary in order to identify potential targets based on the volume of data.

Atlanta Field Office   10/2014 – Present

Currently assigned to investigate cyber crimes, to include computer intrusions.

<u>FBI Assignments</u>

Digital Evidence Extraction Technician (DExT)	12/2011 – Present
Relief Supervisor	04/2010 – Present
Toledo RA, Cleveland	04/2010 – 10/2011
Major Case Coordination Unit, FBIHQ	10/2011 – 10/2014
Cyber Squad, Atlanta Field Office	10/2014 – Present
Coordinator	
Northern Ohio Cyber Crime Task Force	04/2010 – 10/2011
Northwest Ohio InfraGard Chapter	04/2009 – 10/2011

Regal Lager, Inc.
    Information Technology Manager   02/2002 – 11/2007

    Member of the Senior Management Team and responsible
    for the overall technology direction of the company, to
    include long-term goals, policies and procedures. Broad
    range of daily responsibilities included the security,
    availability, configuration and maintenance of the network,
    servers, desktop computers, laptops, mobiles devices and
    corporate software applications; troubleshooting any
    computer related problems; and training personnel on
    systems usage and best practices. Also, developed and
    maintained the company website and ecommerce presence.

Get Functional
    Freelance Consultant   02/2000 – 11/2007

    Worked with companies to improve business processes
    and integrate disparate systems. Developed web sites for
    new web based companies and existing companies creating
    a presence on the Internet for the first time.

Industrial Metal Fabricators, Inc.
    University Cooperative Program   09/1995 – 08/1999

    Responsible for maintaining and supporting the company's
    network, computers and software applications. As part of
    this responsibility, developed and implemented a network
    migration from a Novell coax network to a Windows NT
    10-BaseT network by designing the new network, gathering
    requirements, purchasing equipment and performing the
    migration. Researched, analyzed and coordinated the
    migration from an analog phone switch to an ISDN based
    phone system. Also developed the company's first website.

COMPUTER TRAINING

Microsoft Certified Systems Administrator (MCSA)	
Microsoft Certified Systems Engineer (MCSE)	
Cisco Certified Network Associate (CCNA)	01/2004
Network+ Certification	01/2004
Cyber Special Agent Career Path Stage III Completed	01/2009
Unix Intrusion Techniques	02/2009
Online Covert Employee Certification	03/2009
Image Scan Training	08/2009
Dallas Crimes Against Children Conference	08/2009
A+ Certification	02/2010
Cyber Special Agent Career Path Stage II Completed	02/2010
Advanced Network Investigation Techniques – Windows	03/2010
Basic Innocent Images Training	03/2010
Intrusion Response	07/2010
Dallas Crimes Against Children Conference	08/2010
CART 101 Training	09/2010
AccessData Boot Camp	11/2011
P2P Instructor Training	05/2012

INSTRUCTIONAL EXPERIENCE

U.S. Instruction

Bowling Green State University, Bowling Green, OH	10/2009
Northwest Ohio ISACA Chapter, Bowling Green, OH	01/2011
FBI VCAC International Taskforce Training, Linthicum, MD	08/2012
-P2P file share investigative techniques	
-On-scene triage techniques	
DOJ Project Safe Childhood Conference, Columbia, SC	02/2013
-Anonymization and encryption	
FBI VCAC International Taskforce Training, Alexandria, VA	08/2014
-Investigating Anonymous Networks	

Overseas Instruction

Romanian Directorate for Combating Organized Crime, Romania	06/2011
-P2P file share investigative techniques	
Italian Postal and Communication Police, Italy	03/2012
-On-scene triage techniques	
Italian Postal and Communication Police, Italy	04/2012
-Innocent Images Overview and Techniques	
-On-scene triage techniques	
FBI VCAC International Taskforce Coordination Meeting, Peru	06/2012

Dutch National Police Conference, Netherlands   04/2013
    -Bulletin Board and P2P IP analysis
FBI VCAC International Taskforce Coordination
    Meeting, Netherlands   05/2014

COURTROOM TESTIMONY

United States v. Timothy DeFoggi, District of Nebraska   2014
    Testified as an expert witness regarding the following:
        -Operation of websites and online bulletin boards
        -Computer networking
        -Computer forensics
        -Forensic artifacts pertaining to the use of websites
        -Investigation and analysis of websites and online
        communities dedicated to the exploitation
        of children
        -Methods, tactics and techniques of individuals
        seeking to exploit children online

EDUCATION

Georgia Institute of Technology
    Bachelor of Science, Computer Science   2003

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

UNITED STATES OF AMERICA   )
)
     v.   )   Criminal No. 4:16cr16
)
████████████████████   )

DECLARATION OF DR. MATTHEW MILLER

I, Matthew Miller, declare under penalty of perjury that:

1.   I am an Assistant Professor of Computer Science and Information Technology at the University of Nebraska at Kearney. A copy of my CV is attached to this declaration. Based on my prior work analyzing FBI "Network Investigative Techniques," I have been retained by ████████ 's defense team to speak to the importance of analyzing **all** source code used by the FBI in the deployment of a NIT.

2.   The defense in this case previously submitted a declaration of Vlad Tsyrklevich that was originally drafted and submitted in a related case pending in Washington, *United States v. Michaud*. *See* ECF No. 37-1. I have reviewed Mr. Tsyrklevich's declaration, I agree with and adopt his analysis, and—given my familiarity with both the *Michaud* and *Matish* cases—I consider Mr. Tsyrklevich's declaration to be equally applicable here as it was in *Michaud*.

3.   As explained in the Tsyrklevich declaration, an NIT has four major components. Each of these components must be reviewed and verified by the defense for three basic reasons. First, to ensure that the evidence collected by the NIT is valid and accurate. Second, to ensure that the FBI's use of its NIT did not exceed what was

1

authorized in the NIT search warrant, which is an emerging and serious problem with different types of sophisticated search and seizure technology now used by law enforcement agencies. Third, to develop potential defenses at trial based on the NIT having compromised the security settings on Mr. Michaud's computer and rendering it vulnerable to a host of viruses and remote attacks that would explain to a jury why a defendant's data storage devices may contain child pornography that he or she did not intentionally download.

4.   As the Court is aware, under normal circumstances the FBI would be able to target a specific user on the Internet by using their Internet Protocol (IP) address. This address identifies a user and is allocated to an Internet Service Provider (ISP). The ISP can identify each of their users and then the FBI can investigate that single user.   When users use Tor, they are "anonymized" such that the FBI cannot readily identify them by their IP address because that IP address is not transmitted or shared in any retrievable way. The FBI must use an "exploit" in the software that the user is running on his or her computer to seize the IP address and other identifying information from that target computer directly. An exploit is a piece of software that takes advantage of a flaw in a computer system.   Among other components, the FBI has indicated that it will not produce the exploit that was used in this case. *See* ECF No. 56, 20 n.65.

5.   A computer system that has been exploited has been fundamentally altered in some way. This alteration may cause the computer to crash, lose or alter data, not respond to normal input or it may alter **any of the settings on that system.**[1] Depending on the exploit, it can affect the security posture of the computer going forward.[2]

---

[1] C. Smith, Dangerous Windows 10 flaw lets hackers secretly run any app on your PC, http://bgr.com/2016/04/25/windows-10-applocker-security-issue/, 2016.

[2] D. Goodin, New exploit leaves most Macs vulnerable to permanent backdooring, http://arstechnica.com/security/2015/06/new-remote-exploit-leaves-most-macs-vulnerable-to-permanent-backdooring/, 2015.

2

6.   Once a computer system's security has been compromised, the computer is deemed to have been compromised and vulnerable to attack.

7.   For example, if the security firewall on a computer is disabled by an NIT or other malware, the firewall cannot prevent unauthorized access to the computer by third party attackers and remote computers. Remote attacks on computers are commonplace, with the attackers often automating the process of locating vulnerable computers and targeting them for viruses, remote transmission or storage of illicit materials, and similar misuse. These types of remote computer attacks are so pervasive that it is one of the main reasons that so much time, money and effort is expended by individuals and organizations (including the federal courts) to protect their computers and computer networks from malware.

8.   Without knowing what exploit was used by the FBI in this case, we cannot determine whether the files that the government says were located on the computer were put there by ██████████ .

9.   Moreover, at the suppression hearing in this case, an FBI agent testified for the first time that the NIT collected different pieces of information from a target computer in different ways. Specifically, Agent Alfin testified that target's IP address may not have been collected and sent back to the FBI in a secure, tamper-proof manner. This may mean that the IP address relayed to the FBI was unencrypted and subject to attack by hackers other than the government.   The reliability of the information allegedly transmitted from the target computer to the FBI is a question that I have been asked to help the defense analyze, but I cannot fully determine or opine on the reliability of the transmission without having access to the full NIT source code.

10.   I have had first-hand experience dealing with the complex evidentiary issues that arise when the FBI uses an NIT. I was called upon to analyze a NIT used by the FBI in the Kirk Cottom case that was litigated in federal court in the District of

Nebraska in 2013 and 2014 (Case Number CR13-108). Mr. Cottom was a defendant in the predecessor to "Operation Pacifier" known as "Operation Torpedo." The Court may be familiar with the Cottom case already, as it is referenced in the Defendant's Motion to Compel Discovery and Exhibit 2 to the same. *See* ECF No. 37-2.

11.   Mr. Cottom's defense counsel asked to view the source code that the FBI had used to create the unique identifiers, encrypt identifiers, the NIT and the data logging code. The Government agreed to share **all** of the source code, except for specific code which the FBI reported to the court that it had lost. The binary code for the NIT was provided to our team along with the servers that supplied the NIT. The Government also provided us with access to **all** of the parts system that was used to deanonymize the users of the Tor network. Each time the defense team requested more source code, log files or server code, the Government did not dispute our need to analyze the data and provided us with access to the requested digital resources.

12.   Having all the source code was key to ensuring (among other things also outlined in Mr. Tsyrklevitch's declaration) that the generation of the unique identifiers used for evidentiary data was correct. With the cooperation of the Government during discovery in the Cottom case, we were also able to verify that the NIT only sent back the data that was legally authorized by the search warrant issued in that case, something that remains unknown in Mr. Michaud's case and cannot be resolved by reference to the "data stream" or other fragments of discovery that the FBI is now offering to share.

13.   We were further able to examine in the Cottom case how information was collected by both the NIT server and by the "deanonymizing" server. Perhaps most critically for the defense, we were able to determine what the FBI had or had not done to the security settings on Mr. Cottom's computer and whether a third party attack was an issue in the case. In my opinion, the FBI's unwillingness to produce the same type of NIT discovery in ████████'s case is inconsistent with the government's recognition in

4

the Cottom case that the full NIT source code is relevant and indeed necessary for ▉
▉ to prepare his defense.

DONE this 23rd day of May, 2016.

Dr Matt Miller

Matthew Miller

5

Dr. Matthew James Miller

University of Nebraska at Kearney
Department of Computer Science and Information Systems
Otto Olsen, Room 116E
Kearney, NE USA 68845
Telephone: 308-865-8824

Cell Phone: (785) 410-3526
Email: millermj@unk.edu

Education

Ph.D. Computer Science, Kansas State University, 2012.

M.S. Computer Science, Kansas State University, 2007.

B.S. Computer Science, University of Nebraska at Kearney, 2003.

Employment

Assistant Professor: University Nebraska at Kearney   **2015–Present**

- Courses taught
    - Introduction to programming CSIT-130
    - Computer Organization CSIT-301
    - Operating Systems CSIT-401
    - Software Engineering CSIT-404
    - Computer Security CSIT-458
    - Reverse Engineering CSIT-499
- Student projects
    - Developing a secure medical application for viewing Continuity of Care Documents

Consultant: Milhous Ink, LLC. Independant Contractor   **2014–Present**

- Reverse Engineering a flash based Network Investigation Technique (NIT) developed by the FBI for de-anonymizing TOR end nodes Case Number 8:13-cr-00108-JFB-TDT Doc # 227-1 https://s3.amazonaws.com/s3.documentcloud.org/documents/2124281/fbi-tor-busting-227-1.pdf

Training/Certificates:

- Red Team Hunting DakotaCon 2016
- Advanced Penetration Testing DakotaCon 2015
- Advanced Reverse Engineering Black Hat Las Vegas 2014
- Malware Analysis DakotaCon 2014

Assistant Professor: Dakota State University   **2012–2015**

- Courses taught with Online sections
    - Introduction to programming I CSC-150
    - Introduction to programming II CSC-250
    - Object Oriented Design CSC-260
    - Assembly CSC-314

Dr. Matthew James Miller   2

- Reverse Engineering CSC-444
- Operating Systems CSC-456
- Android Development CSC-492
- Algorithm Analysis CSC-705
- Advanced Reverse Engineering for Ph.D. students CSC-844

○ Service at Dakota State University
- Served as the Vice-president of General Faculty
- Helped develop the Applied Computer Science masters program
- Created a local programming contest
- Increased attendance of our ACM programming contest from 3 teams to 7 teams
- Taught at a 2 Coed Cybersecurity camp for high school students
- Taught at a 1 Girls Cybersecurity camp for high school students
- Worked on the Red-Team at the North Central CCDC Competition

○ Student Research Projects at Dakota State University
- Created parallel password cracking software; abstract accepted at NCUR
- Developed a method of detecting and mitigating ROP attacks in software
- Developed Android applications for members of the community

○ Advising 50+ students per semester about Computer Science and Cybersecurity

Programmer: The Onyx Collection   **2007–2013**

○ Created an online ordering system that handles $1+ million in sales per month
○ Developed software to manage electronic order forms, electronic catalogs, product entry and product assembly
○ Created an open source library for java to database interaction

NSF GK-12 Fellow: Kanas State University   **2010–2012**

○ Developed lessons for high school students that integrate sensory technology into the classroom
- Sensors included Wiimotes, Android phones, Lego MindStorms, Lego NXT, Wii Balance board, GPS Devices, Kinect and Cameras
○ Taught lessons for Physical Education and Enhanced Learning Education
○ Participated in outreach for other areas of Kansas (Dodge City, Wamego, Rock Creek)

Writer: The Master Teacher   **2010–2012**

○ Developed and wrote lesson plans for educators that explains classroom technology integration
- Topics included programming using OpenGL, Wiimotes in weightlifting, photography and Android application development

ESSI outreach program speaker: Kanas State University   **2008–2012**

○ Introduced middle school students to robotics and the use of computer science in society

EXCITE outreach program: Kansas State University   **2005–2012**

○ Developed curriculum for introducing female high school students to programming and robotics

Dr. Matthew James Miller 3

  ○ Coordinated, managed and taught the program to the high school students

Research Assistant: Kansas State University   **2006–2008**

  ○ Researched porting of shell scripts for SANDIA Turbo SIP from Linux to Windows

  ○ Developed a distributed software system for the estimation of impact of irrigation on the Great Plains Aquifer in western Kansas

  ○ Researched and developed an installer for porting the SANDIA Turbo SIP from Linux to OS X Leopard

  ○ Developed a system for model checking the GMoDS goal model

Teaching Assistant: Kansas State University   **2004–2006, 2008-2010**

  ○ Developed curriculum and taught computer science class for non-programmers (CIS 111)

  ○ Taught the lab portion for the Introduction to Computer Science class (CIS 200)

  ○ Acted as a Teaching Assistant for the Computers and Society (ethics) class (CIS 415)

  ○ Acted as a Teaching Assistant for the Concurrent Programming class (CIS 625)

Teacher for the Research Experience for Teachers (RET): Kansas State University **2004–2005**

  ○ Taught curriculum to high school teachers that involved both hardware and software

Adjunct Instructor: University of Nebraska at Kearney   **Fall 2003**

  ○ Taught 1 section of CS-130

Course development at Dakota State University

○ I redeveloped the assembly language class (CSC-314) to use an open source assemble that can be used for free on a linux server. The course was developed to lead directly into the reverse engineering course.

○ I developed the reverse engineering course (CSC-444). This course is designed to meet the rigorous standards provided by the NSA. This course is key to the Center of Excellence designation that has been awarded to DSU.

○ I developed the graduate reverse engineering course (CSC-844). This course is designed as the foundation for the PHD in Cybersecurity.

Works in Progress

Shadow Return a ROP Mitigation tool.

Analysis of FBI Network Investigative Tools

Publications

Tom Bulatewicz, Daniel Andresen, Stephen Welcha, Wei Jina, Sanjoy Dasb, and Matthew Miller. A software system for scalable parameter estimation on clusters. In *Proceedings of the 8th LCI International Conference on High-Performance Clustered Computing*, 2007.

Tom Bulatewicz, W Jin, S Staggenborg, S Lauwo, M Miller, S Das, D Andresen, J Peterson, David R Steward, and SM Welch. Calibration of a crop model to irrigated water use using a genetic algorithm. *Hydrology and Earth System Sciences*, 13(8):1467–1483, 2009.

Scott A DeLoach and Matthew Miller. A goal model for adaptive complex systems. *International Journal of Computational Intelligence: Theory and Practice*, 5(2):83–92, 2010.

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Norfolk Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	CRIMINAL NO. 2:16cr92
	)	
██████████████,	)	
	)	
Defendant.	)	

GOVERNMENT'S RESPONSE TO DEFENDANT'S MOTION TO COMPEL

Now comes the United States of America, by and through attorneys, Dana J. Boente, United States Attorney for the Eastern District of Virginia, and Elizabeth M. Yusi, Assistant United States Attorney, and submits its response in opposition to the defendant ████████ ████████'s Motion to Compel Discovery. For the reasons set forth below, the defendant's motion should be denied.

INTRODUCTION

Defendant ██████████████ ("the defendant") is charged in this case with receipt of child pornography. The charges arise from an investigation into Playpen, a website through which registered users like the defendant regularly accessed illegal child pornography. That website operated on the Tor network. This network allows its users to mask their Internet Protocol ("IP") addresses, which—absent such concealment—ordinarily can be used to identifying website users. The Tor network operates to conceal this information by bouncing user communications around a network of computers before transmitting such communications to their ultimate destination. The defendant's IP address was discovered through the court-authorized use of Network Investigative Technique ("NIT"). Pursuant to a search warrant authorized in this District, Playpen's content—which was hosted on a computer server located

within the district—was augmented with additional computer instructions comprising the NIT

while the website briefly operated under government control.[1]

The defendant seeks disclosure of what he generally describes as the "source code or

programming code for the NIT" and "the unique identifier generator" used to identify his

computer. Def.'s Mot. to Compel Disc. at 1. Defendant does not meet the Fourth Circuit

standard for materiality and incorrectly relies on the Ninth Circuit standard in his materiality

claim. Moreover, even if the Court were to find that disclosure of the NIT programming code

was material to his defense, that information is protected by a qualified law enforcement

privilege. Accordingly, this Court should deny the defendant's motion.[2]

BACKGROUND

I. Procedural History

On June 22, 2016, a federal grand jury sitting in Norfolk returned a five-count indictment

charging the defendant with four counts of receipt of child pornography, in violation of 18

U.S.C. § 2252(a)(2), and one count of possession of child pornography, in violation of 18 U.S.C.

§ 2252(a)(4). At his arraignment, the Court set a preliminary motions deadline of July 29, 2016,

and a trial date of October 18, 2016.

---

[1] Further detail about the website, investigation, and NIT is contained in the government's
Response to the Defendant's First Motion to Suppress and exhibits thereto (ECF 19). Such
information is incorporated here by reference.

[2] Just as with defendant's First and Second Motions to Suppress, defendant's motion contains
the identical factual and legal arguments as those contained in Motions to Compel filed in this
Court in other related cases. *See United States v. Matish*, 4:16cr16 (J. Morgan), *United States v.
Darby*, 2:16cr36 (J. Doumar), and *United States v. Eure*, 2:16cr43 (J. Doumar). In each of these
cases, the court conducted evidentiary hearings. Both Judge Doumar and Judge Morgan issued
lengthy opinions denying the defendants' motions to compel. *See United States v. Matish*, ---
F.Supp.3d ---, 2016 WL 3545776 (attached as Exhibit A). Attached as Exhibit B is the court
order in the *Eure* and Darby cases. Attached as Exhibits C and D are transcripts of the
evidentiary hearings in *Matish* and *Darby/Eure.*

II. Discovery Requests and the government's Responses

On July 1, 2016, the parties entered an agreed discovery order. ECF 11. The government

provided discovery pursuant to that order. Among the items included in that disclosure were

materials pertaining to the investigation such as investigative reports and forensic report

regarding the defendant's digital devices. On July 29, 2016, defense counsel requested by letter

additional discovery items related to information related to Playpen and its users and disclosure

of the NIT source code. Ex. E (letter from A. Conner to E. Yusi dated July 29, 2016). That

same day, government responded. Ex. F (letter from E. Yusi to A. Conner dated July 29, 2016).

Regarding the defendant's request for discovery, the government advised that the

information sought did not consist of evidence the government intended to use in its case-in-

chief at trial and that such information had not been obtained from and did not belong to the

defendant. Ex. F. The government further advised that it did not believe—and the defendant

had failed to indicate why—that information was material to his defense. *Id*. The government

also advised that the investigative technique is subject to law enforcement privilege, which the

government asserted. *Id*. The government noted that the information collected through the use

of the court-authorized NIT is available for counsel's review and would remain available for

further review during the pendency of the litigation. *Id*. The government also offered to provide

the defendant a copy of that information subject to the entry of a protective order. *Id*.

Additionally, regarding the NIT results, the government explained that only a limited set

of information was collected through court-authorized use of the NIT; specifically, the

information described in Attachment B of the warrant authorizing the deployment of the NIT, as

reflected in the user report that has been provided to counsel. The government clarified that

other information about user activity, such as the pages and postings accessed, had been

collected through request data and website logs that were not a function of the NIT. *Id.* In this

response, the government offered to make additional information available to the defendant,

including an offline copy of Playpen that would enable the defense team to navigate through

pages of the website as a user could when the website was online. *Id.*

LAW AND ARGUMENT

Defendant has not shown why the information he seeks is material to either his pretrial

motions or to his defense. Moreover, the information that the defendant seeks to compel is

subject to a qualified law enforcement privilege.

I.   The Defendant has Failed to Show that the NIT Programming Code is Material to his Defense

Under Federal Rule of Criminal Procedure 16, a criminal defendant has a right to inspect

documents, data, or tangible items within the government's "possession, custody, or control,"

that are "material to preparing the defense." Fed. R. Crim. P. 16(a)(1)(E). "[I]n the context of

Rule 16, 'the defendant's defense' means the defendant's response to the government's case in

chief." *United States v. Armstrong*, 517 U.S. 456, 462 (1996). "[E]vidence is material as long as

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. Caro, 597 F.3d 608, 621 (4th Cir. 2010) (quoting *United States v. Lloyd*, 992

F.2d 348, 351 (D.C. Cir. 1993)).

The defendant bears the burden of showing that information sought under Rule 16

"would . . . actually help[] prove his defense." *Id.* To show materiality under Rule 16 "[t]here

must be some indication that the pretrial disclosure of the disputed evidence would have enabled

the defendant to significantly alter the quantum of proof in his favor." *Id.* (quoting *United*

States v. Ross, 511 F.2d 757, 763 (5th Cir. 1975), cert. denied 423 U.S. 836). A defendant

cannot meet this burden through "general description[s] of the information sought" nor through

"conclusory allegations of materiality." *Id.* (quoting *United States v. Mandel*, 914 F.2d 1215,

1219 (9th Cir. 1990)). In fact, "[w]ithout a factual showing there is no basis upon which the

court may exercise its discretion, and for it to ignore the requirement is to abuse its discretion."

Mandel, 914 F.2d at 1219. "[O]rdering production by the government without any preliminary

showing of materiality is inconsistent with Rule 16." *Id.* Moreover, Rule 16 does not authorize

a defendant to embark on a fishing expedition, which is exactly what the defense requests

amounts to. *See United States v. White*, 450 F.2d 264, 268 (5th Cir. 1971); *United States v.*

Rigmaiden, 844 F. Supp. 2d 982, 1002 (D. Ariz. 2012); *United States v. Delacruz*, No. Case 14

Cr. 815 (KBF), 2015 WL 2211943, at *1 (S.D.N.Y. May 12, 2015) ("Rule 16 does 'not entitle a

criminal defendant to a 'broad and blind fishing expedition among [items] possessed by the

government on the chance that something impeaching might turn up.'" (quoting *United States v.*

Larranga Lopez, No. 05 Cr. 655 (SLT), 2006 WL 1307963, at *8 (E.D.N.Y. May 11, 2006)

(alteration in original)); *United States v. Sandoval*, No. CR 04-2362 JB, 2006 WL 4079018, at *2

(D. N.M. Jun. 8, 2006) (finding that information a defendant sought was "not material under rule

16, but rather appear[ed] to be an attempt at a fishing expedition to find material that might lead

to some cross-examination at trial").

    Brady v. Maryland, 373 U.S. 83 (1963), requires that under the Due Process Clause, the

government shall disclose "evidence favorable to an accused upon request…where the evidence

is material either to guilt or to punishment. *Caro*, 597 F.3d at 619. Materiality depends on a

"reasonable probability that, had the evidence been disclosed to the defense, the result of the

proceeding would have been different." *Id.* In the Fourth Circuit, a reasonable probability must

be "sufficient to undermine confidence in the outcome." *Id.* *Brady* is not in place to be used as a

discovery device. *Id.* When a defendant can only guess as to what requested materials may

expose, it does not satisfy *Brady*'s requirement that the evidence be favorable to the defendant.

Id. To determine materiality, a court must determine if the evidence withheld from the defense

"reasonably could be considered as placing the entire case in such a different light that

confidence in the verdict is undermined." *Waters v. Clarke*, 2012 U.S. Dist. LEXIS 140762 *17

(E.D.Va. 2012).

The defendant seeks a copy of the NIT programming code for three stated reasons: (1)

"so that [his] computer forensics expert can independently determine the full extent of the

information the government seized from [his] computer when it deployed the NIT," (2) "whether

the NIT interfered with or compromised any data or computer functions," and (3) "whether the

government's representations about how the NIT works are complete and accurate." Def.'s Mot.

to Compel at 1. He contends that the information is relevant to his First and Second Motions to

Suppress, yet does not explain why the discovery he seeks will help him answer any of the

questions he claims, in those motions and the instant motion, must be answered. *Id.* He presents

no factual information whatsoever in support of his speculative assertions and fails to show

materiality regarding any of the specified reasons for the seeking the requested information.

Indeed, the information sought by the instant motion is not relevant to any of the suppression

motions currently pending before the Court.[3] The latter motions challenge the sufficiency and legality of the search warrant.

For all of the reasons set forth below, the defendant has also failed to show the materiality to his defense of the information he seeks. Accordingly, to the extent the Court excuses the defendant's failure to timely file the instant motion, it should nevertheless deny it.

A. The defense does not accurately apply the materiality standard for the purposes of Fed. R. Crim. P. 16.

█████████████ interpretation of the materiality standard is broad and incorrect in light of Fourth Circuit precedent. As noted above, the Fourth Circuit's standard for materiality is that, "evidence is material as long as 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." *Caro*, 597 F.3d at 621. However, ████████ directs the court's attention to a similar case currently being litigated in the United States District Court for the Western District of Washington at Tacoma, where the judge found that the defense had shown that the NIT source code was material to preparing the defense. Def. Mot. to Compel Disc. pp. 3-4. In the Ninth Circuit, evidence is "material" under Rule 16 if it is helpful to the development of a possible defense. *United States v. Olano*, 62 F.3d 1180, 1203 (9th Cir. 1995). A defendant must make a "threshold showing of materiality" in order to compel discovery pursuant to Rule 16(a)(1)(E). *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir. 1995).

---

[3] The defendant filed two motions to suppress challenge the sufficiency and legality of the search warrant (and in a very limited sense, the execution of the warrant). This latter question concerns only whether the triggering condition—logging in to Playpen—occurred. Neither of the defendant's motions challenge the extent of the information identified by the NIT or the NIT's technical aspects, operation, or functionality—either generally or with respect to the defendant, specifically. Accordingly, the NIT source code and an independent forensic analysis of the same are neither relevant nor necessary to the Court's determination of the pending motions.

"Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the government is in possession of information helpful to the defense." *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990).

Although the defense asserts that the *Michaud* court clearly found materiality, the different standards between the circuits warrant a different outcome in ▮▮▮▮▮▮▮'s case.[4] The Fourth Circuit's requirement that there is a "strong indication that [the material] will play an important role" in the defense is narrower than the Ninth Circuit's condition that the defendant show a "possible defense." For the reasons stated above, ▮▮▮▮▮▮ is initiating a fishing expedition in which he seeks to obtain information that he either already has through the computer instructions or has alternative means of obtaining on his own. While this may satisfy the "possible defense" standard in the Ninth Circuit, the information already made available to him during discovery clearly precludes him from arguing that the entire NIT source code is material in the Fourth Circuit.

▮▮▮▮▮▮'s reliance on the case out of the Ninth Circuit is flawed because the standard is different in the Fourth Circuit. The materiality standard to be applied in his case does not encompass anything that might help his defense. As discussed *infra*, the defendant has not shown a strong indication that the evidence will play an important role in finding evidence, helping witnesses, corroborating testimony, or aiding in impeachment or rebuttal.

---

[4] Following a government motion to reconsider its discovery order in *Michaud* and review of *ex parte*, *in camera* materials submitted by the government, that court determined that the government was not required to turn over the further information pertaining to the NIT that ▮▮▮▮▮▮ now requests. *United States v. Jay Michaud*, No. 15-cr-5351, ECF 205 (W.D. Wa. May 18, 2016). That court did not reconsider its finding of materiality, however, and later entered an order excluding the NIT evidence and its fruits. *Id.*, ECF 212. However, that decision is being appealed by the government to the Ninth Circuit Court of Appeals. *Id.*, ECF 213.

B. Additional discovery to what the government has already provided will not shed light on the accuracy of the identifying data that connects ███████ to both the "Slutwhore" account and specific activity on the Playpen website.

████████ contends that, pursuant to Rule 16, he is entitled to the NIT source code because such information may reveal the accuracy of the data the government used to identify ████████ on the Playpen Website. For ████████ to obtain such information, he would have to show that disclosure would "alter the quantum of proof in his favor." *See Caro*, 597 F.3d 608, 621. In other words, ████████ bears the burden of showing that the information he seeks will raise doubt that the NIT accurately identified him as the individual accessing and downloading child pornography. The government will provide ████████ with the computer instructions that generated the identifying data, and the identifying data, additional requests fall outside the scope of appropriate discovery outlined in *Brady*.[5] *See id.* (citing *Brady* and stating that materiality depends on whether the result of the proceeding would be different after disclosing the information to the defendant); *see also White*, 450 F.2d at 268 (deeming requests outside the scope of appropriate discovery as prohibited fishing expeditions). Therefore, additional discovery requests regarding the government's chain of custody of the NIT are cumulative and unnecessary.

---

[5] In *Michaud*, the defense similarly moved to compel production of the NIT programming code and the government opposed disclosure, as it does here. Prior to the hearing on that motion, the government offered—without conceding any obligation to do so—to make available for review at an FBI facility, the instructions sent to and executed on Michaud's computer, which produced the NIT results. *See* Gov't Resp. to Def.'s Mot. to Compel at 4, *Michaud*, 3:15cr05351, ECF 134 (W.D. Wash. Jan. 21, 2016). The defense agreed and information was provided to the defense pursuant to a protective order, including a copy of the computer instructions sent to Michaud's computer that, when executed, produced the NIT results, the NIT results themselves, the date and time the NIT was executed on Michaud's computer, and the Playpen thread that Michaud was accessing when the NIT was executed. *Id.* at 1, 4. Without conceding any obligation to do the same in light of the defendant's untimely request and his similar failure to show materiality, the government is willing to make the same information available to the defendant in this case. The government strenuously opposes disclosure of any additional information described in Tsyrklevich and Miller's declaration, as it has consistently done in *Michaud*.

First, █████'s fundamental misunderstanding of the NIT's basic structure

misinforms his perception of how the NIT processed and transmitted the data that identified him

as a Playpen user. Relying on both the Tsyrklevich and Miller declarations, ████ asserts

that the NIT is comprised of four components, all of which he claims are necessary to determine

the accuracy of the identifying information. *See* Decl. of Dr. Matthew Miller (hereinafter,

"Miller Decl.") ¶ 3. Of the alleged four components, he claims there is an "exploit," a

"payload," software that generates the payload and injects a unique identifier into it, and a server

that stores the delivered information. *See* Decl. of Tsyrklevich (hereinafter, "Tsyrklevich Decl.")

¶ 4. In reality, the NIT is one component, which is the computer instructions delivered to

█████'s computer that gathered his identifying information after he logged into the Playpen

website. Ex. G, Decl. of Special Agent Daniel Alfin(hereinafter, "Alfin Decl.") ¶ 5[6]. As noted

before, those instructions, and the information obtained via their execution, will be made

available for review. *Id.*

Particularly, ████ seeks disclosure of the "exploit" in order to determine whether

the government "executed additional functions outside the scope of the NIT warrant."

Tsyrklevich Decl. p. 3. However, even assuming that the NIT does have multiple components,

the "exploit" is not relevant to anything found in the warrant; it would only show how the NIT

was deployed to █████'s computer, not what it did once it began interacting with his

computer. Alfin Decl. ¶ 12. Furthermore, the defense's contention that the "exploit" could have

made changes to █████'s computer is purely theoretical. Alfin Decl. ¶ 14. While it is

possible for some exploits to do so, the NIT in question and the exploit it used to deliver

---

[6] While Special Agent Alfin's declaration was originally drafted for the related case, *United States v. Matish*, 4:16cr16, before Senior United States District Judge Henry Coke Morgan, the same information applies in this case.

computer instructions did not do so. *Id.* The defense experts point to no evidence that the NIT

initiated any changes to █████████'s computer system or security firewall that would warrant

concern that the identifiers misidentified █████████ as a Playpen user. *Id.* To alleviate

█████████'s concerns about the "exploit," the government will offer to allow the defense to

review the two-way network data stream transmitted to the FBI from █████████'s computer

after the NIT's deployment. Alfin Decl. ¶ 15. Reviewing the data stream would show the

defense that the data sent from █████████'s computer is identical to the data the government

provided as part of discovery. Alfin Decl. ¶ 16.

Additionally, █████████ requests the "server component," but this is unnecessary

because there are alternative means of verifying the accuracy of the NIT information. Alfin

Decl. ¶ 18. The government agrees to provide a copy of the data stream sent by █████████'s

computer to the government as a result of the NIT, so defense experts do not need to access

government servers at all. Alfin Decl. ¶ 19. Once the copy is provided to the defense, the

defense expert can compare the information sent to the government by the NIT to the

information provided in discovery to determine whether the material the government recorded

from █████████'s computer is in fact what was sent by █████████'s computer. *Id.* The

government has confirmed that the information sent to the government from █████████'s

computer is exactly what the government will disclose in discovery as obtained by the NIT. *Id.*

Lastly, █████████ demands the computer code that "generates the payload and injects an

identifier" in order to contest the legitimacy and uniqueness of the identifier used to find him.

Tsyrklevich Decl. p. 3. However, this is unnecessary information because a unique identifier is

incorporated into the NIT upon each deployment. When the user's computer activates the NIT

and sends information to the government, the unique identifier accompanies the information.

11

82

Alfin Decl. ¶ 26. ▓▓▓▓▓▓▓s speculation concerning the existence of duplicate unique

identifiers and the accuracy of the NIT information is unfounded, because all identifiers received

by the government matched those that the government generated without any duplicates. Alfin

Decl. ¶ 26. In fact, a review of the FBI database containing the information gathered by the NIT

revealed that: (1) there are no duplicate unique identifiers within the database, so each identifier

assigned to each Playpen user was unique, (2) the identifier associated with "Slutwhore" was

unique, and (3) only identifiers generated by the NIT were in the database, which means that no

outside entity tampered with the identifiers used in the Playpen investigation. Alfin Decl. ¶ 27.

The defendant has not proven that disclosure would alter the quantum of proof in his

favor and therefore has not proven that any further information is material to his defense. The

information he seeks will not raise any suspicion that the NIT did not accurately identify him as

the person accessing child pornography. The government will provide the defendant with

identifying data and everything he needs to answer his questions regarding accuracy and

identification. Additional discovery requests do not assist him in his pursuit of these questions,

and therefore his motion to compel should be denied.

**B. The requested discovery also has no bearing on ▓▓▓▓▓▓▓'s claim that someone
or something else may have been responsible for the downloading of child
pornography on his device.**

▓▓▓▓▓▓▓'s expert Miller speculates about the possibility that the NIT disabled

▓▓▓▓▓▓▓'s computer security, and, accordingly, argues the possibility that the NIT may have

opened the door for other entities to download illicit material onto his computer without his

knowledge. Miller Decl. ¶¶ 6-8. To obtain the source code and subsequently present to the jury

that the child pornography came from some other source, ▓▓▓▓▓▓▓ must show that the

requested discovery holds a "reasonable probability that, had the evidence been disclosed to the

12

defense, the result of the proceeding would have been different." *Caro*, 597 F.3d at 619. This would be a difficult argument considering ████████'s confession to collecting child pornography. And, if ████████ is only guessing as to what the materials may provide, then *Brady*'s requirement that the material must be favorable to the defendant is not satisfied. *Id*. at 619. In ████████'s case, the entire source code is not material to his defense because the evidence does not indicate the possibility that ████████ unknowingly obtained child pornography.

To be malware, a software or computer program must set out to make "malicious" changes to a computer's security settings or systems. The NIT did not deploy any program that would have made changes to ████████'s computer; it merely interacted with his computer to obtain the information that traced him to the "Slutwhore" account. Alfin Decl. ¶ 6. Further, after the NIT sent instructions to ████████'s computer, it ceased interaction and left no residual openings that would allow the government to return for further access to that computer. Alfin Decl. ¶ 8. Outside of pure speculation regarding a theoretical possibility, ████████ points to no facts to suggest otherwise.

Should the defense decide to further inquire about any potential malware that could have been left on ████████'s computer, his devices are available for review. Alfin Decl. ¶ 35. However, the defense has declined to review the network data, which would be a valuable tool for searching for malware. Alfin Decl. ¶ 32. Alternative to inspecting the source code itself, there are other ways to find malware on a device that would help the defense identify other malware that may have led to the unintentional downloading of child pornography. Alfin Decl. ¶ 33 and 34. For example, an investigator may find all files and programs with unknown purpose and find its function to determine whether they are malware. Alfin Decl. ¶ 33. Additionally, the

13

investigator can conduct a dynamic analysis on devices suspected of containing malware by

creating copies of all suspect files and executing them in test environments to determine their

functions. Alfin Decl. ¶ 34. ███████'s devices, as available to the defense, are appropriate

subjects for both malware-testing techniques described above. Alfin Decl. ¶ 35. Therefore, the

defense does not need the source code to determine whether malware was responsible for the

collection of child pornography found on ███████'s computer rather than ███████ himself.

The defendant has not shown that the discovery he requests holds a reasonable

probability that if it were to be disclosed, the results of the proceeding would be different.

███████only speculates so to what the materials might reveal, and thus *Brady*'s requirement

that the material in fact be favorable to him is not satisfied. Because the defendant has not met

the requirements for further discovery, his motion to compel should be denied.

C. The extent of the information seized from the defendant's computer

As explained in the NIT search warrant affidavit and as the government has disclosed, the

NIT programming code consists of computer instructions that caused a user's activating

computer to deliver certain authorized information to a computer controlled by the government.

E.g., Gov't Resp. to Def.'s First Mot. to Supp., Ex. I at 24-26, ¶¶ 33-34. Review of the

programming code is unnecessary to determine the extent of information seized from the

defendant's computer by operation of the NIT because the information collected by the NIT is

available to the defense, and that information answers this question. It includes the defendant's

IP address, a unique identifier generated by the NIT to distinguish the data from other computers,

information about whether the NIT had already been delivered to the computer, and the

computer's operating system, "Host Name," active operating system username, and Media

Access Control ("MAC") address. That information is contained in the "user report" available to

14

the defendant, should the defendant contact the government to view the information as offered in

the government's letter. Ex. F. The collection of all such information was authorized by the NIT

warrant.

The defendant fails to provide any factual support regarding what other information he

suggests might have been collected through the NIT, let alone other information that was

collected.[7] Indeed, the defendant has not even asked the government whether any information

was collected by the NIT beyond that described in the warrant and reflected in the user report.

The answer is no. Regardless, even if the NIT had collected further information, only that

information could be subject to suppression as outside the scope of the warrant—not the

information specifically authorized by that warrant. Because, however, there is no such further

information, there is nothing to suppress and no compelling need for an expert to independently

determine the information obtained via the NIT.

The defendant also fails to provide any information to this Court to meet his burden of

showing why or how review of the programming code, as opposed to reviewing the information

collected by the NIT (or other information the government could provide) would answer any

---

[7]   Nothing in the defendant's motion or the witness declarations he attaches claims, for example, that the computer instructions would have collected information other than what the government disclosed they did. Nor does he even identify what supposed other information might have been collected. Rather, the declaration's author posits, after having reviewed the computer instructions comprising the NIT, "whether the payload that has been provided was the only payload associated with the NIT or whether other payloads were executed" and claims that he needs to analyze and understand additional information to determine whether the information provided in discovery "was the only component executing and reporting information to the government" and/or "whether [that additional information] executed additional functions outside the scope of the NIT warrant." Tsyrklevich Decl. at 3. This speculation is wholly irrelevant to the matter at hand. The results provided to the defendant consist of the only information collected by the NIT. Even if some unspecified additional information had been collected by the NIT (or some other set of computer instructions), the defendant does not claim that this unspecified information bears on this case. Nor could he, because the only NIT information relied on by the government in the warrant for the defendant's home and that it may rely on at trial is that which has already been disclosed.

15

question about what information the NIT collected. Indeed, the defendant has not asked for any

information related to the use of the NIT and the information it collected, beyond that already

offered by the government, which might have enabled him to assess the questions he now claims

compel production of the NIT programming code. Accordingly, he fails to show how review of

the programming code would reveal the full extent of the information the government seized

from ███████'s computer – particularly in light of the fact that the information collected by

the NIT has already been disclosed. The defendant therefore fails to make any showing of

materiality or to present facts that tend to show the government is in possession of information

helpful to the defense.

D. Whether the NIT interfered with or compromised any data or computer functions

Review of the programming code is also not material for the purpose of determining

whether the NIT interfered with or compromised any data or computer functions. The defendant

presents no information to support this wholly speculative hypothesis. Nor can he. The

defendant has not made any discovery requests for information concerning the operation of the

NIT beyond the information already offered by the government, other than his request for the

NIT programming code and the NIT results. In the instant motion, he fails to provide any

information regarding what he means by "interfer[ing] with or compromis[ing] any data or

computer functions." Def.'s Mot. to Compel Disc. at 1. He also does not explain how, if such

interfering with or compromise of data or computer functions did occur—and it did not—this

fact would lead to suppression of any evidence, since the only evidence "seized" was authorized

by the warrant. Nor has the defendant made any showing of how review of the programming

code would provide information to support an argument for some other sort of relief if the NIT

did interfere with or compromise any data or computer functions. Finally, he has not shown the

16

impact of any such interference or compromise on any defense to the charges pending against

him. Indeed, he cannot do so, because, as the government has disclosed, the conduct on which

the indictment is based relates to the defendant's activities on the Internet that were discovered

on the defendant's computer media found at his residence (and that he confessed to during an

interview with law enforcement).

Critically, the defendant has ongoing access to the forensic examination conducted of his

computer and other digital devices seized. He has also been provided with substantial

information pertaining to his dates of access to the pertinent website, and the date and time at

which the NIT identified his IP address accessing the site. Despite having that information, he

presents nothing to this Court from any examination of his devices to support his rank

speculation that the NIT could have interfered with or compromised any data or computer

functions, let alone that it did. Nor has the defendant ever asked to perform an independent

forensic examination of his computer or other digital devices. Absent some indication—based in

fact as opposed to speculation and conjecture—that the NIT interfered with or compromised any

data or computer functions—something the government disputes occurred—the defendant fails

to present any facts tending to show that the government possesses information that "would . . .

actually help[] prove his defense." *Caro*, 597 F.3d at 621.

E. Whether the government's representations about how the NIT works in its warrant applications were complete and accurate

Review of the programming code is also not material for the purpose of determining

whether representations about how the NIT works are complete and accurate. By its nature, this

is an entirely speculative request that any defendant could make, at any time, in any case, in an

effort to justify any request for information from the government. The defendant presents no

facts to suggest that the government is in possession of any information helpful to the defense on

that issue. Nor does he even claim that the NIT worked other than as described, just that he

needs to verify that its actual operation comported with that description. Such rank speculation

cannot support a finding of materiality. *Id*. In fact, this sort of speculative request turns the

criminal discovery process on its head. If the standard for obtaining criminal discovery were,

"What if the government's representations were not correct or complete," then there would be no

limitation to criminal discovery and every defendant would be entitled to fish through every

scrap of information in the government's possession in order to look for something that might

impeach a government representation. That is inconsistent with the disclosure requirements

established by Rule 16, *Brady*, and *Giglio*.

With respect, specifically, to the descriptions of the NIT set forth in the search warrant

affidavit,[8] the defendant has not identified any facts to suggest that those descriptions, in

particular, are incomplete or inaccurate, despite having received substantial information

pertaining to the use and execution of the NIT warrant on his computer, specifically—including

exactly where on the website he was (a posting thread in the kinky fetish – zoo subforum) when

he received the NIT. He also has access to the forensic examination of the devices seized from

his home and has not requested to conduct any independent examination of those devices. Even

having all of this, the best the defendant can do is hypothesize that the NIT could have worked

other than as described. He cannot even muster an explanation as to what, if any, description of

the NIT he is unable to test. A defendant can always allege, absent factual support, that it is

arguably possible that the government did not include complete and accurate information in a

---

[8] In describing how the NIT would operate, the NIT affidavit explained that when a user's
computer accessed Playpen and downloaded its content in order to display web pages on the
user's computer, that content would be augmented with additional computer instructions (which
comprised the NIT) that, once downloaded to a user's computer would cause the user's computer
to transmit the information specified in the warrant. Gov't Resp. to Def.'s First Mot. to Supp.,
Ex. I, at 24, ¶ 33.

search warrant. A mere allegation simply will not supply a basis for seeking to rummage

through the government's files. *See Caro*, 597 F.3d at 621. Indeed, "[w]ithout a factual showing

there is no basis upon which the court may exercise its discretion" to require discovery on this

point, and for the Court to ignore that requirement, as the defendant wishes it to do, "is to abuse

its discretion." *Mandel*, 914 F.2d at 1219.

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.

Rather he merely speculates that such a review might produce information that could impeach

the NIT warrant or testimony concerning the process by which he was identified. "Mere

speculation that *Brady* material exists does not justify fishing expeditions in government files."

United States v. Paulino, 1996 U.S. App. LEXIS 30032, at *4 (4th Cir. Nov. 20, 2006); *see also*

United States v. Crowell, 586 F.2d 1020, 1029 (4th Cir. 1978); *United States v. Brown*, 360 F.3d

828, 833 (8th Cir. 2004) ("[M]ere speculation that materials may contain exculpatory evidence is

not . . . sufficient to sustain a *Brady* claim); *United States v. American Radiator & Standard*

Sanitary Corp., 433 F.2d 174, 202 (3d Cir. 1970) ("[A]ppellants' mere speculation about

materials in the government's files [does not require] the district court or this court under *Brady*

to make the materials available for their inspection."). Absent the required factual showing, the

defendant's request amounts to nothing more than a fishing expedition, which is not sanctioned

by Rule 16 or any other law.

The defendant contends that the government's disclosure of information in other cases is

relevant to the inquiry in this case. First, the defendant points to one related case in which a

court *initially* ordered the government to disclose information related to the NIT programming

code. Def.'s Mot. to Compel Disc. at 3 (citing Order Granting Third Mot. to Compel Disc.,

United States v. Michaud, Crim. No. 3:15cr05351, ECF 161 (W.D. Wash. Feb. 17, 2016)). In

that case, the government—as it does here—vigorously objected to disclosure of the NIT

programming code; litigation concerning such disclosure is ongoing. *See* Minute Entry for

Proceedings, *Michaud*, Crim. No. 3:15cr05351, ECF 199 (W.D. Wash. May 12, 2016).

Defendant fails to note that, as discussed *supra*, after the government moved for reconsideration

of the court's order and an *in camera*, *ex parte* hearing, the court reversed its earlier ruling and

declared that the government was not required to produce the requested discovery concerning the

NIT programming code, including the items described in Vlad Tsyrklevich's Jan. 13, 2016

Declaration. Nothing about the government's conduct in that litigation is inconsistent with the

position the government has taken in this case.

The defendant also contends that the government's disclosure of information pertaining

to a different network investigative technique in an unrelated case is inconsistent with the

government's position concerning the disclosure of the NIT in this case. It is not. The *Cottom*

case in the District of Nebraska, No. 13-cr-108, involves a different investigation of a different

website using a different investigative technique than the one pertinent to the defendant's case.

That investigative technique was publicly sourced and no longer in use—in fact, example

programming code for the technique was available for review on a public website. After the

completion of suppression hearings and before trial, the government disclosed, in an expert

notice, information about government expert witnesses, including details about the specific

investigative technique used in that case, about which those experts were to testify at trial. The

government did not, in that case, as it does here, challenge whether defendants had met their

burden to demonstrate materiality related to the disclosed information. Further, there—unlike

here—the government did not assert that the particular technique was subject to law enforcement

privilege, see infra, as that technique was publicly available.

Although the defendant sets forth three purposes for which he seeks disclosure of the NIT

programming code, he fails to identify any facts that he claims establish the materiality of that

information to his suppression motions or to his defense. Nor has the defendant shown that the

government's objection to disclosure is inconsistent with its conduct in other cases.

II. None of the Defendant's Other Claims of Relevance Establish Materiality

The defendant suggests that review of the NIT programming code is necessary to

"investigate the chain of custody for data collected remotely by the NIT." Def.'s Mot. to

Compel Disc. at 2. This request is again purely speculative—he presents no facts whatsoever to

suggest that there are or were any issues with the so call "digital 'chain of custody'" pertaining to

the NIT-derived information. That the NIT-derived information is computer-related information

does not entitle the defendant or his expert to rummage through government files—digital or

otherwise—in the hope of finding an error in the chain of custody. *Cf. United States v. Guzman-*

Padilla, 573 F.3d 865, 890 (9th Cir. 2009) ("[M]ere speculation about materials in the

government's files [does not require] the district court . . . under *Brady* to make the materials

available for [appellants'] inspection."); *Am. Radiator & Standard Sanitary Corp.*, 433 F.2d at

202 (same).

III. The NIT Programming Code is Subject to Qualified Law Enforcement Privilege

If the Court finds—as it should—that the defendant has failed to meet his burden to show

that the requested information is material and otherwise discoverable under Rule 16, that will

resolve the defendant's motion. In the event the Court were to determine that the NIT

programming code is material to ████████'s defense, however, then the requested information

21

92

pertaining to that code is nevertheless subject to a qualified law enforcement privilege, as its

disclosure would be harmful to the public interest.[9] Specifically, disclosure could diminish the

future value of important investigative techniques, allow individuals to devise measures to

counteract these techniques in order to evade detection, discourage cooperation from third parties

and other governmental agencies who rely on these techniques in critical situations, and possibly

lead to other harmful consequences not suitable for inclusion in this response. Ex. H, Affidavit

of Robert Stone (filed under seal) (hereinafter Stone Aff.) [10] ¶5. As explained below, courts have

generally recognized that, because of the sensitivity of information that may support this type of

privilege claim, it is appropriate to consider a submission from the government *ex parte* and *in*

camera. Accordingly, in the event it determines the defendant's request for programming code

is material, the United States accordingly requests that the Court permit the United States to offer

evidence in support of its privilege claim *ex parte* and *in camera*.[11]

The privilege has its roots in *United States v. Roviaro*, where the Supreme Court first

recognized a qualified "informer's privilege" that protects the identity of government informants.

353 U.S. 53, 59 (1957). Courts have since extended the qualified privilege in *Roviaro* to cover

---

[9] Further, the FBI has derivatively classified portions of the tool, the exploits used in connection with the tool, and some of the operational aspects of the tool in accordance with the FBI's National Security Information Classification Guide. As of the date of this filing, the government is waiting on a formal, signed document from an FBI Original Classification Authority to detail the specific aspects of the classification of the information.

[10] While the Stone declaration was originally drafted for the related case*, United States v. Matish*, 4:16cr16, before Senior United States District Judge Henry Coke Morgan, the same information applies in this case.

[11] Should the Court permit the *ex parte* and *in camera* submission, the government advises that a Classified Information Security Officer with the Litigation Security Group at the U.S. Department of Justice will have to assist in providing certain documents to the Court. Arranging for this may cause a short delay, and the government requests the Court's indulgence in arranging such an event.

other investigative techniques, including traditional and electronic surveillance. For example, in *United States v. Green*, the D.C. Circuit applied the privilege to bar disclosure of the location of an observation post in a drug investigation because failing to do so would "likely destroy the future value of that location for police surveillance." 670 F.2d 1148, 1155 (D.C. Cir. 1981). In *United States v. Van Horn*, the Eleventh Circuit applied the privilege to bar disclosure of the nature and location of electronic surveillance equipment because disclosure would "educate criminals regarding how to protect themselves against police surveillance." 789 F.2d 1492, 1507 (11th Cir. 1986); *see also In re The City of New York*, 607 F.3d 923, 928-29 (2d Cir. 2010) (finding that the district court erred by failing to apply the privilege to reports made by undercover agents because they contained "detailed information about [] undercover operations," disclosure of which would "hinder [law enforcement's] ability to conduct future undercover investigations"). The purpose of the privilege is, among other things, "to prevent disclosure of law enforcement techniques and procedures." *In re Dep't of Investigation*, 856 F.2d 481, 484 (2d Cir. 1988); *Commonwealth of Puerto Rico v. United States*, 490 F.3d 50, 64 (1st Cir. 2007).

The government bears the initial burden of showing that the law enforcement privileges applies to the materials at issue, *In re The City of New York*, 607 F.3d at 944, and the courts then apply a balancing test in determining whether disclosure is required, *Van Horn*, 789 F.2d at 1508. To meet its initial burden, the government must show that the materials contain information that the law enforcement privilege is intended to protect, which includes "information pertaining to law enforcement techniques and procedures, information that would undermine the confidentiality of sources, information that would endanger witnesses and law enforcement personnel [or] the privacy of individuals involved in an investigation, and information that would otherwise . . . interfere[] with an investigation." *In re The City of New*

York, 607 F.3d at 944 (citations and internal quotation marks omitted); *see also Commonwealth of Puerto Rico v. United States*, 490 F.3d 50, 64 (1st Cir. 2007) (extending privilege recognized for "confidential government surveillance information" to "law enforcement techniques and procedures"). *See* Stone Aff. ¶ 6.

Because the evidence required to establish the privilege is often sensitive, courts have recognized that it is appropriate to permit the government to make its showing through an *ex parte* and *in camera* evidentiary hearing, the record of which should be sealed for later review. *See, e.g.*, *United States v. Johns*, 948 F.2d 599 (9th Cir. 1991) (approving, over the defense objection, court's consideration of the government's request to maintain the confidentiality of an informant in an *ex parte*, *in camera* hearing); *United States v. McLaughlin*, 525 F.2d 517, 519 (9th Cir. 1975) (upholding trial court's conducting of *in camera* hearing regarding disclosure of informant's identity and determining that disclosure was not required); *United States v. Fixen*, 780 F.2d 1434, 1439-40 (9th Cir. 1986) (suggesting use of *in camera* proceedings to resolve law enforcement privilege issues); *United States v. Kiser*, 716 F.2d 1268, 1273 (9th Cir. 1983) (remanding to district court to conduct *ex parte*, *in camera* hearing pertaining to *Roviaro* privilege issue and citing cases authorizing *in camera* hearings in similar situations); *Van Horn*, 789 F.2d at 1508 (district court held *in camera* hearing); *Global Relief Found, Inc. v. O'Neill*, 315 F.3d 748 (7th Cir. 2002) ("*Ex parte* consideration is common in criminal cases where, say, the identity of information might otherwise be revealed"); *In re Department of Homeland Security*, 459 F.3d 565, 569-71 (5th Cir. 2006) (instructing the district court in a civil case to "review the documents at issue *in camera* to evaluate whether the law enforcement privilege applies"); *In re The City of New York*, 607 F.3d at 949 (determining requesting party did not have compelling need for requested information based on *in camera* review of the documents);

24

Rigmaiden, 844 F. Supp. 2d at 982 (denying defendant's requests for discovery concerning investigative technique after *ex parte*, *in camera* review at which the court heard the government's reasons for nondisclosure); *cf. In re Grand Jury Proceedings #5 Empanelled Jan. 28, 2004*, 401 F.3d 247, 253 (4th Cir. 2005) (approving the use of *ex parte* and *in camera* review of allegedly privileged documents in the context of a crime-fraud exception claim).

At an *ex parte in camera* hearing, the United States can provide a more detailed presentation about both the nature of the information that the defendant is requesting and the government's concerns regarding its disclosure. Because of the sensitivity of the technique and for other reasons, simply filing the material under seal with a protective order is inadequate to address the government's concerns. Indeed, courts have recognized that sealing documents and materials containing such sensitive information is frequently inadequate to prevent its public disclosure. *See, e.g., In re The City of New York*, 607 F.3d at 937-39 (citing numerous specific examples of instances where "sealed" materials were inadvertently or intentionally disclosed, and concluding that "[i]n light of how often there are all-too-human lapses with material filed 'under seal'" that it could not "conclude with confidence that filing" the sensitive information would adequately protect the information from public disclosure).

Upon a finding that the privilege applies, there is a "pretty strong presumption against lifting the privilege." *In re The City of New York*, 607 F.3d at 945 (*quoting Dellwood Farms v. Cargill*, 128 F.3d 1122, 1125 (7th Cir. 1997)). The burden shifts to the defendant, who must show that his need for the information overcomes the public interest in keeping it secret. *See Alvarez*, 472 F.2d at 113 (finding, regarding disclosure of informer identity, that "in balancing the interest of the government against that of the accused, the burden of proof is on the defendant to show the need for disclosure); *see also Van Horn*, 789 F.2d at 1507. The public interest in

keeping the information private must be balanced against a defendant's articulated need for the information. *See Roviaro*, 353 U.S. at 628-29. "Whether a proper balance renders nondisclosure erroneous must depend on the particular circumstances of each case, taking into consideration the crime charged, the possible defenses, the possible significance of the [privileged information], and other relevant factors." *Id*. at 629.

In conducting this balancing, the court should consider the defendant's "need [for] the evidence to conduct his defense and [whether] there are . . . adequate alternative means of getting at the same point. The degree of the handicap [to the defendant] must then be weighed by the trial judge against the policies underlying the privilege." *United States v. Harley*, 682 F.2d 1018, 1020 (D.C. Cir. 1982); *United States v. Cintolo*, 818 F.2d 980, 1002 (1st Cir. 1987) (the question is "whether the [defendant] demonstrate[s] an authentic 'necessity,' given the circumstances to overbear the qualified privilege); *United States v. Foster*, 986 F.2d 541, 543 (D.C. Cir. 1993) (balancing the defendant's need for information against importance of government's interest in avoiding disclosure).

In striking this balance, the Court should also keep in mind that the need for disclosure is more limited in the context of a suppression hearing than at trial. *See McCray v. Illinois*, 386 U.S. 300, 311 (1967); *see also Rigmaiden*, 844 F. Supp. 2d at 990 (applying *McCray* in the context of motion for disclosure of electronic tracking equipment). Even if the party seeking disclosure successfully rebuts the presumption (by a showing of, among other things, a "compelling need"), the court must still then weigh the public interest in non-disclosure against the need of the litigant for access to the privileged information before ultimately deciding whether disclosure is required. *In re the City of New York*, 607 F.3d at 948.

As can be explained in more concrete terms in an *ex parte*, *in camera* hearing, the public

interest in nondisclosure here significantly outweighs the defendant's need for the information,

particularly in light of the defendant's speculative claims regarding the materiality of the

requested information. In particular, the risk of circumvention of an investigative technique if

information is released has been recognized as a factor in applying law enforcement privilege to

electronic surveillance. *See Van Horn*, 789 F.2d at 1508.[12] Accordingly, in the event the Court

finds the requested information to be material, the Court should hold an *ex parte*, *in camera*

hearing to assess the applicability of the privileges and the defendant's need for the materials.

The analysis of the Sixth Circuit in *United States v. Pirosko*, 787 F.3d 358 (6th Cir. 2015)

is instructive here. *Pirosko* affirmed the district court's denial of a motion to compel disclosure

of "the law enforcement tools and records" (there, ShareazaLE, a proprietary program used

exclusively by law enforcement) used to search a defendant's computer for child pornography.

787 F.3d at 362. Similar to this case, the defendant in that case presented a purported expert

declaration claiming that analysis of the government's investigative tools "can determine

whether law enforcement officers manipulated data on the subject computer [or] the error rates in

records used." *Id*. at 363. The defendant also contended that review of the source code was

necessary to allow "his experts to determine whether [the software] gives government officials

'the ability to manipulate settings or data on the target computer (even unintentionally),'

'whether the software allows agents to override shared settings to download files that a normal

---

[12] Risk of circumvention has also been accepted by numerous courts as a basis for nondisclosure in the civil FOIA context. *See, e.g., James v. U.S. Customs and Border Protection*, 549 F. Supp. 2d 1, 10 (D.D.C. 2008) (concluding that CBP properly withheld information under FOIA that "could enable [others] to employ measures to neutralize those techniques"); *Judicial Watch v. U.S. Department of Commerce*, 337 F. Supp. 2d 146, 181-82 (D.D.C. 2004) ("[E]ven commonly known procedures may be protected from disclosure if the disclosure if the disclosure could reduce or nullify their effectiveness.")

user would not be able to download,' and 'the error rate' associated with the software." *Id*. at

365. As here, the defendant produced no evidence to suggest that any of those speculative

concerns were actually manifested – such as, through an examination of the defendant's

computers. The government objected to disclosure on both Rule 16 materiality and law

enforcement privilege grounds, arguing that granting the motion to compel "would compromise

the integrity of its surveillance system and would frustrate future surveillance efforts." *Id*. at

365. The Court of Appeals for the Sixth Circuit endorsed the government's argument on both

points, holding that "it is important for the defendant to produce some evidence of government

wrongdoing" – which that defendant had failed to do – when balancing the government's

assertion of the law enforcement privilege against the needs articulated by a defendant. *Id*. at

365-66 (emphasis supplied).

Similarly persuasive is the District Court's analysis in *United States v. Rigmaiden*. In

that case, the government, acting on the authority of a tracking device warrant, used a cellular

site simulator in order to locate a wireless "aircard" that assisted in locating and ultimately

identifying the defendant. [13] The defendant moved to compel production of additional

information pertaining to the technology, methods, and personnel involved in tracking the

"aircard." The government provided information pertaining to the aircard tracking, but opposed

disclosure of technical details, asserting law enforcement privilege. Following hearings related

to the issues, the Court denied the defendant's requests, finding either they were speculative and

accordingly, not material, or that the defendant had not demonstrated a compelling need in light

of the government's persuasive showing regarding the law enforcement privilege. *Rigmaiden*,

844 F. Supp. 2d at 996-1004.

---

[13] An "aircard" may be attached to a laptop in order to provide Internet service.

Here, the defendant cannot demonstrate any compelling need for the requested information. As demonstrated above, his requests are entirely speculative and conclusory. Such requests are insufficient to justify a compelling need, in light of the government's assertion of privilege. *See United States v. Buras*, 633 F.2d 13566, 1360 (9th Cir. 1980); *Guzman-Padilla*, 573 F.3d at 890. The defendant cannot compel disclosure based simply on his conjecture that privileged material may contain something relevant.

In addition, the 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 the information is relevant. *Harley*, 682 F.2d at 1020. The government is willing to provide, as it did in *Michaud*, the computer instructions comprising the NIT that, when executed, produced the NIT results. This information would allow defendant to verify that the particular instructions would have produced the particular results and therefore that the NIT was properly described and operated consistent with that description. Defendant also has a copy of the forensic report of his computer and substantial information pertaining to his dates of access to the pertinent site and the date and time at which the NIT identified his IP address accessing that site. He may analyze that information if he wishes to verify that the NIT did not interfere with or compromise any data or computer functions. And, to the extent the defendant wishes to request chain of custody documentation from the government regarding items to be admitted at trial, there are numerous avenues available for him to request such information short of seeking to rummage through the government's files or to compel the government to disclose privileged material. Accordingly, the defendant cannot establish the sort of compelling need required to outweigh the significant public interest in nondisclosure of additional materials pertaining to the use and execution of the court-authorized NIT.

29

100

<u>CONCLUSION</u>

For the foregoing reasons, the defendant's motion to compel should be denied.

Respectfully submitted,

DANA J. BOENTE
UNITED STATES ATTORNEY

By:_____/s/_____
Elizabeth M. Yusi
Assistant United States Attorney
Attorney for the United States
United States Attorney's Office
101 West Main Street, Suite 8000
Norfolk, Virginia 23510
Phone: (757) 441-6331
Fax: (757) 441-6678
Email: elizabeth.yusi@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Norfolk Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 2:16cr92
	)	
███████████	)	

**DEFENDANT'S REPLY TO GOVERNMENT'S RESPONSE TO
DEFENDANT'S MOTION TO COMPEL**

███████████, through counsel and pursuant to Federal Rule of Criminal Procedure

47(F)(1), respectfully submits this Reply to the Government's Response to Defendant's Motion

to Compel, ECF No. 21.

*   *   *

The defense asks the Court to order the government to provide the exploit and unique ID

generator for the NIT it used to search ███████b's computer. Here, the defense first

responds to the government's attempt to distinguish the recent decision in *United States v.*

Michaud. Second, the defense addresses the fundamental flaw in the government's position:

namely, that the government attempts to avoid *producing* evidence by instead *describing*

evidence and unilaterally asserting the inferences that the government's agents believe can be

drawn therefrom. And, third, the defense provides the attached declaration of Dr. Christopher

Soghoian of Yale Law School and the ACLU as a factual response to the government's

declarations.

***Michaud* Court Found Requested Data Material to the Defense**

The government suggests that the decision in *Michaud*—involving the exact same

discovery request related to the exact same investigation—is not instructive for two reasons.

First, the government claims that there is a meaningful difference in Rule 16's materiality

1

standard that renders the requested data material in the Ninth Circuit but immaterial in the Fourth. (ECF No. 21, 8.) This is a red-herring. For the reasons discussed below, the Fourth Circuit's materiality standard is met here.

Second, the government directs the Court away from reliance on *Michaud* because, at the time the government filed its Response, "litigation concerning such disclosure is ongoing." (ECF No. 21, 20.) This is apparently an allusion to the fact that the government is appealing the district court's suppression of all NIT-related evidence in *Michaud* based on the government's failure to produce material discovery related to the government's use of NIT malware. In the order attached to the underlying Motion as Exhibit E (and for the reasons stated in open court in the transcript included as part of the same exhibit) the district court in *Michaud* suppressed all fruits of the NIT search in light of the government's refusal to provide the material data. The *Michaud* court held that even though the requested data was subject to a qualified law enforcement privilege, the data was sufficiently important to the defense that the government could not proceed with a prosecution that relied on this evidence without producing it. The *Michaud* litigation (in the district court) is over, the government's appeal to the Ninth Circuit notwithstanding. The Court here should reach the same conclusion as the Court in *Michaud* as the facts are identical and the law is not meaningfully different.

Rule 16 Gives the Defense a Right to Inspect; Not a Right to FBI Observations and Assurances

The government repeatedly insists that the defense declarations and motions lack specificity; it calls the defense request a "fishing expedition." (ECF No. 21, 5.) This is patently false. The fundamental disagreement here is whether Rule 16 requires the defense to take the government's word for it when, 1) the defense requests evidence, 2) the defense articulates clearly the relevance of that evidence to its defense, and 3) the government insists that it has reviewed the evidence and

assures the defense that, in its view, the evidence will not fundamentally alter the quantum of proof at trial.

The government relies heavily on a declaration by FBI Special Agent Daniel Alfin. (ECF No. 21-7.) In essence, Agent Alfin's declaration is a series of statements in which he suggests that he has conducted a review of the evidence. Rather than producing the evidence, the government provides Alfin's analysis of what the evidence shows. This is a fundamental misconception of the adversarial system. ███████ and his attorneys—with the help of experts hired by the defense— are entitled to review the evidence itself to determine what technological defenses can and cannot be made at trial.   To avoid a battle-of-the-experts at trial, the government is proposing that the defense take the government-expert's word for what the evidence shows. Indeed, the government's seeks to preclude defense experts from even looking at the facts and data underlying the opinions set forth in the government-experts' declarations.

This phenomenon is revealed by the government's position regarding the discoverability of the exploit. The government concedes that exploits like the one the government used here *can* infect a computer and leave the computer vulnerable to other security compromises. *See, e.g.*, ECF No. 21- 1, ¶¶ 9, 14; ECF No. 21 ("While it is possible for some exploits to [make changes to the computer], the NIT in question and the exploit it used to deliver computer instructions did not do so."). Indeed, Alfin concedes that what the defense expert, Dr. Miller, described as the basis for a technical trial defense: It is "theoretically possible" for an exploit like this to compromise the security of a firewall. *Id.* at ¶ 14. But then Aflin assures the defense that the exploit the FBI used against ███████ not compromise his computer's security. How is Agent Alfin so sure of this? Agent Alfin testified as to the basis for the assertion in Paragraph 14 of his declaration in a recent evidentiary hearing:

```
 5   Q.  Let's talk about the exploit, then.

 6          Do you have the technical capability to write an

 7   exploit?

 8   A.  I do not.

 9   Q.  Did you work at all in the creation of the exploit in

10   this case?

11   A.  I did not.

12   Q.  You've obviously testified, both here and in your

13   declaration, about what the exploit does and doesn't do,

14   correct?

15   A.  Yes, I have.

16   Q.  Is that based on your review of the exploit?

17   A.  It is based on my use of the exploit.

18   Q.  Okay.  And you make that clarification because you've

19   never actually reviewed the exploit, correct?

20   A.  Are you referring to the source code of the exploit?

21   Q.  Well, have you looked at the source code of the exploit?

22   A.  I have not.
```

(ECF No. 21-4, 111:5-22.)[1] Agent Alfin continued:

---

[1] At an evidentiary hearing in the *Matish* case, Agent Aflin testified for the first time that he had never reviewed the exploit: "I have not viewed the exploit myself, nor have I ever claimed to or made any implication that I have." (ECF No. 21-3, 31:18-19.)

```
10   BY MR. GRINDROD:

11   Q.  So you've not reviewed the exploit in this case.  Is that

12   correct?

13   A.  I have not reviewed the exploit source code in this case.

14   Q.  And all of the statements you're making about what the

15   exploit does and doesn't do, those statements are based on

16   your observations of running the exploit.  Is that correct?

17   A.  In part, yes.

18   Q.  What else are they based on?

19   A.  Based on my conversations with other people who are

20   knowledgeable in the matter, as stated in my declaration.

21   Q.  Who are those people?

22   A.  Other FBI personnel.

23   Q.  Yeah, but what people?

24   A.  That information is subject to law enforcement privilege.
```

(ECF No. 21-4, 112:10-24.) Finally, SA Aflin explained:

```
4        The part of your statement in which you say this

5   exploit specifically didn't make fundamental changes, is that

6   based on your personal observations or based on what other

7   FBI agents have told you?

8   A.  I tested a NIT on a computer -- or, rather, the exploit

9   on a computer under my control.  I observed that it did not

10   open up any security holes on it, it didn't place any files

11   on it, it didn't make it any more vulnerable to outside

12   attackers.  It is based on my observations and my testing.

13   Q.  And how many times did you run the exploit before you

14   reached that conclusion?

15   A.  A few times.  I don't know the exact number.

16   Q.  More than five?

17   A.  Possibly.  Less than a hundred.

18   Q.  Was it less than ten?

19   A.  It may have been.
```

(ECF No. 21-4, 115:4-19.)

5

In sum, Agent Alfin does not possess the expertise to write the exploit.   He has never actually reviewed the exploit.   And the conclusory statements he offers in his declaration are based on some combination of conversations with unidentified government agents and Agent Alfin having "run" the exploit possibly less than 10 times while looking for obvious changes.   Agent Alfin may be misinformed.   He may simply lack the sophistication (or incentive) to find such properties in the FBI's exploit.   But, in any event, the government's fundamental position is that an FBI agent's *description* of the exploit and *assurances* about its properties are sufficient to eliminate the government's obligation to produce it. [2]

The government attempts to take the same approach with respect to discovery related to the "unique identifier."   Agent Alfin's declaration purports to answer the "ultimate question" posed by the defense by stating, "I have reviewed the list of unique identifiers … and confirmed that there were in fact no duplicate[s]".   ECF No. 21-7, at ¶ 26.   But this conclusion without any underlying evidence deprives the defense of a meaningful ability to cross-examine government witnesses at trial. Not only has the government refused to produce the code that generates the "unique identifiers" it has refused to produce what the code generated or a more meaningful description of the process: Again, Agent Alfin's testimony at a recent hearing is illuminating.   When asked about how he knows that the government's code did not create duplicate identifiers, Agent Alfin testified:

---

[2] The government's assertion that a forensic review of ▇▇▇▇▇▇▇▇▇'s computer could serve as an adequate substitute for production of the exploit is erroneous.   Dr. Soghoian addresses this argument both in his declaration and in his testimony in the *Darby* and *Eure* cases. *See* Def. Ex. F; *see also* Gov't Ex. D, ECF No. 21-4, 53:6-54:4.   The government's assertion that "the defense has declined to review the network data" is simply false. (ECF No. 21, 13.)   In the ▇▇▇▇▇▇ case, the government has not yet made the so-called "network data" available.   But in other Playpen cases where the government has actually produced this data, the Office of the Federal Public Defender has reviewed it.   And—for the reasons explained by Dr. Soghian—it is not a substitute for the discovery the defense seeks.

```
4   A.   It's a very simple process.   You put every unique
5   identifier in a spreadsheet, and you say "find duplicates"
6   and the spreadsheet says there are no duplicates.   It's very
7   simple to do.
8   Q.   Have you produced that spreadsheet to the defense?
9   A.   No.   I have provided the unique identifier used in the
10  matter at hand.
11  Q.   And even if you're not providing the code that created
12  the unique identifier, to your knowledge, has the government
13  produced any indication as to how that unique identifier was
14  even created?
15  A.   Yes, we generated unique identifiers.
16  Q.   Using an algorithm?
17  A.   Yes.
18  Q.   Did you write that algorithm?
19  A.   I did not.
20  Q.   Do you know that algorithm?
21  A.   I do not.
22  Q.   Would you recognize it if you were presented with it?
23  A.   I would not.
24  Q.   Can you explain the inner workings of how that algorithm
25  works?
```

```
                           D. Alfin - Cross
1   A.   I can.   It generates a unique identifier.
```

(ECF No. 21-4, 103:4-104:1.)   Under the Fourth Circuit's decision in *United States v. Caro*,

evidence "is material as long as 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." 597 F.3d 608, 621 (4th Cir. 2010) (quoting *United States v.*

Lloyd, 992 F.2d 348, 351 (D.C. Cir. 1993)).   Without the government producing the exploit and

the unique ID generator, how exactly is the defense supposed to prepare its own trial expert to

challenge the government on whether the "unique identifier" allegedly associated with ▮

██████ really was unique or instead could have been a duplicate associated with some other Playpen user? How can the defense corroborate whether the exploit made fundamental changes to ██████'s computer that rendered it vulnerable to unauthorized access by actors who were perhaps less "well-intentioned" than the FBI? And how can ██████'s lawyers hope to impeach or rebut Agent Alfin and other government witnesses at trial when they testify about evidentiary material that neither ██████'s lawyers nor his tech experts have ever seen?

Due process and Rule 16 require that the actual items—the *evidence*—be produced and made available for inspection by the defense. Agent Alfin's entire declaration is an attempt to substitute *descriptions* of evidence for the *production* of evidence. *See, e.g.,* ECF No. 21-7, at ¶ 19 ("I have reviewed that data stream and, as explained below, confirmed…"); *id.,* at ¶ 9 ("I have personally executed the NIT on a computer under my control and observed…"). This is simply not what Rule 16 contemplates.

Dr. Soghoian's Declaration in Response

Finally, the defense submits here a declaration by Dr. Christopher Soghoian of Yale Law School and the ACLU, which responds to some of the factual issues raised by Agent Alfin's declaration. *See* Ex. F. To be sure, the government's current monopoly on the evidence allows its agents to review the very data at issue. But, together, Mr. Tsyrklevich, Dr. Miller, and Dr. Soghoian have provided the Court with substantial evidence in support of the defense's position that the requested data is essential to mounting a technology-based defense to this technology-dependent prosecution. The Court should require the government to stop using its asymmetry of information as both a sword and a shield. The defense respectfully requests that the Court compel production.

Respectfully submitted,

██████████████████

By:_____/s/_____

Amanda C. Conner
VSB # 88317
Attorney for ███████████
Office of the Federal Public Defender
150 Boush Street, Suite 403
Norfolk, Virginia 23510
(757) 457-0816
(757) 457-0880 (telefax)
amanda_conner@fd.org

Andrew W. Grindrod
VSB # 83943
Assistant Federal Public Defender
Attorney for ███████████
Office of the Federal Public Defender
150 Boush Street, Suite 403
Norfolk, Virginia 23510
(757) 457-0800
(757) 457-0880 (telefax)
andrew_grindrod@fd.org

9

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

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal No. 4:16cr16
	)	
██████████████████	)	

DECLARATION OF DR. CHRISTOPHER SOGHOIAN

I, Christopher Soghoian, declare the following under penalty of perjury:

1. I am a researcher focused on privacy, computer security and government surveillance. I completed a B.S. in Computer Science from James Madison University, a M.S. in Security Informatics from The Johns Hopkins University and a Ph.D. in Informatics from Indiana University. My academic research has been published in a number of law journals, and has been cited by several federal and state courts, including by the 9th Circuit Court of Appeals and the State Supreme Courts of New Jersey and Massachusetts.[1]

2. I am currently employed by the American Civil Liberties Union as the Principal Technologist in the ACLU's Speech, Privacy and Technology Project. I am also a visiting fellow at Yale Law School's Information Society Project. I have previously worked in technical roles at the Federal Trade Commission, Google, Apple, and IBM. I have written this declaration as an unpaid volunteer expert for the defense and submit it to the court in my personal capacity, not on behalf of my employer.

3. I have researched the FBI's use of Network Investigative Techniques ("NITs") for more than three years. In 2014, I organized the first-ever academic conference in the United States focused on hacking by law enforcement, held at Yale Law School.[2] I have given several public talks about the use of hacking and malware by the FBI, including at training events for federal judges organized by the Federal Judicial Center.

---

[1] *See US v. Pineda-Moreno*, 617 F. 3d 1120, Court of Appeals, 9th Circuit 2010 (Kozinski dissental), *State v. Earls*, 70 A. 3d 630 - NJ: Supreme Court 2013 and *Commonwealth v. Augustine*, 467 Mass. 230 - Mass: Supreme Judicial Court 2014.

[2] *See* Law Enforcement and Hacking, Information Society Project, Yale Law School, February 18, 2014, videos online at https://www.law.yale.edu/yls-today/yale-law-school-videos/hacking-technologies-used-law-enforcement and
https://www.law.yale.edu/yls-today/yale-law-school-videos/legal-and-policy-implications-hacking-law-enforcement
.

1

4. In 2014, while researching the history of FBI hacking, I discovered that in a 2007 operation, FBI agents impersonated the Associated Press in an effort to deliver surveillance software to a teenager in Timberline, Washington. My subsequent public disclosure of this information resulted in significant news coverage, a formal complaint to the Attorney General from twenty-five news organizations,[3] a Congressional probe into the incident,[4] and a public defense of the practice by the FBI Director.[5]

Network Investigative Techniques

5. As Special Agent Alfin's declaration makes clear, there is some disagreement between Michaud's technical experts and the FBI about what a NIT is and is not. There is also clear disagreement about whether or not a NIT is "malware".

6. The term "Network Investigative Technique" was created by the US government. While researching the history of NITs, I was informed by a senior DOJ official that the term originated in the Computer Crime and Intellectual Property Section within DOJ's Criminal Division.

7. Outside of the law enforcement community, a number of terms of art are used by technical security experts to describe software that is installed without the knowledge and consent of a computer user, and that covertly extracts information from that person's computer. These terms include "malware," "surveillance software," and "Remote Administration Tools" (RATs). These terms are all functionally equivalent.

8. In his declaration, Special Agent Alfin suggests, without citing any supporting evidence, that an essential component of malware is that the software must make permanent changes to the security settings of the target computer.[6] I disagree with this statement.

9. The Ninth Circuit Court of Appeals has described malware as software that "works by, for example, compromising a user's privacy… stealing identities, or spontaneously opening Internet links to unwanted websites…." *See Zango v. Kaspersky Lab, Inc., 568 F.3d 1169 (9th Cir. 2009).* Like the malware in *Zango,* the NIT used by the FBI in the Playpen

---

[3] *See* The Reporters Committee for Freedom of the Press *et al.*, Letter to Eric H. Holder, Jr. and James B. Comey, Jr., November 6, 2014, http://www.rcfp.org/sites/default/files/2014-11-06-letter-to-doj-fbi-regarding-se.pdf
[4] *See* Senator Patrick Leahy, Letter to Eric Holder Jr., October 30, 2014, http://thehill.com/sites/default/files/10-30-14_leahy_to_holder_re_-_fbi_fake_ap_article.pdf.
[5] See James B. Comey, To Catch a Crook: The F.B.I.'s Use of Deception (Letter To The Editor), New York Times, November 5, 2014, http://www.nytimes.com/2014/11/07/opinion/to-catch-a-crook-the-fbis-use-of-deception.html
[6] *See* Alfin Declaration, paragraph 6, page 2.

2

investigation compromised the privacy and anonymity of the individuals that visited the site, and forced their web browsers to connect to an unwanted site (the FBI's server in Virginia).

10. The capabilities of NITs used by the FBI in other cases include identical surveillance features as malware used by criminals and foreign governments. These capabilities include being able to remotely activate the webcam and microphone on a victim's computer.[7]

11. The FBI has used the same methods as those used by criminal hackers and foreign governments to deliver malware to targets. This includes the impersonation of journalists[8] and the delivery of malware to large numbers of visitors to a particular website (a technique that experts call a "watering hole attack").[9]

12. The primary difference between the FBI's NITs and the malware used by hackers and authoritarian foreign governments appears to be that the FBI's software is used pursuant to court orders issued by a court in the United States. From a technical perspective, NITs are still malware.

---

[7] Compare the features of BlackShades, a malware tool used by criminals to the capabilities of the NIT software used by the FBI. *See US v. Yücel*, 97 F. Supp. 3d 413 - Dist. Court, SD New York 2015 ("The malware included a remote access tool ('RAT'), which enabled users 'to remotely control victims' computers, including [by] captur[ing] the victims' keystrokes as they type'—the 'keylogger' function— 'turn[ing] on their webcams, and search[ing] through their personal files.'") *See also* Ellen Nakashima and Craig Timberg, FBI's search for 'Mo,' suspect in bomb threats, highlights use of malware for surveillance, Washington Post, December 6, 2013 ("The most powerful FBI surveillance software can covertly download files, photographs and stored e-mails, or even gather real-time images by activating cameras connected to computers, say court documents and people familiar with this technology.")

[8] *See* Bill Marczak and John Scott-Railton, Keep Calm and (Don't) Enable Macros: A New Threat Actor Targets UAE Dissidents, Citizen Lab, Munk School of Global Affairs, The University of Toronto, May 29, 2016, https://citizenlab.org/2016/05/stealth-falcon/ (describing attempts by an entity, believed to be the government of the United Arab Emirates, attemping to deliver malware to dissidents by pretending to be a fictious journalis).

[9] *See* Michael Mimoso, Council on Foreign Relations Website Hit By Watering Hole Attack, IE Zero-Day Exploit, Threatpost, December 29, 2012, https://threatpost.com/council-foreign-relations-website-hit-watering-hole-attack-ie-zero-day-exploit-122912/77352/ . The Department of Justice has taken the position that bulk delivery of NITs in operations like Playpen are not watering hole attacks. As with the question of whether a NIT is malware, the Department of Justice and the technical community do not see eye to eye. *See* David Bitkower, Deputy Assistant Attorney General, Memorandum to Reena Raggi, Chair, Advisory Committee on Criminal Rules, December 22, 2014 http://www.uscourts.gov/file/17944/download at 145 ("The ACLU calls this technique a 'watering hole attack' and suggests that it may violate the Fourth Amendment... The Department disagrees both with that label and with the legal conclusion.")

3

The Importance Of Encryption

13. When an individual browses the web, data that is transmitted from their computer to the websites they visit must pass through communications networks and networking equipment run by a number of Internet Service Providers. These Internet Service Providers all have the ability to inspect and modify that data as it passes through their network. Internet Service Providers may modify the contents of web pages that are being delivered through their network, in order to to inject advertisements or to facilitate advertising-related tracking of their customers.[10]

14. In addition to the authorized parties that can intercept and tamper with data as it flows over the Internet, unauthorized parties can do so too, if they have hacked into a server or network that the data passes through. For example, journalists relying on documents from NSA whistleblower Edward Snowden have revealed that Britain's signals intelligence agency hacked into a number of Belgian and German communications networks in order to intercept the communications that flowed through those networks.[11]

15. When individuals use an open, or poorly secured, WiFi network, it is trivially easy for hackers in the vicinity to inspect and modify data that is being transmitted over that WiFi network.[12]

16. In order to protect their customers from a number of privacy and cybersecurity threats, including the interception and tampering of private user data, many major Internet companies use an encrypted connection to protect data that is transmitted to and from their

---

[10] *See* Gabi Nakibly *et al.*, Website-Targeted False Content Injection by Network Operators, 25th USENIX Security Symposium,, August, 2016, http://www.cs.technion.ac.il/~gnakibly/papers/arXiv1602.07128.pdf. *See also* Nate Anderson, How a banner ad for H&R Block appeared on apple.com—without Apple's OK, Ars Technica, April 8, 2013, http://arstechnica.com/tech-policy/2013/04/how-a-banner-ad-for-hs-ok/. *See also In the Matter of Cellco Partnership, d/b/a Verizon Wireless*, Federal Communications Commission, March 7, 2016, EB-TCD-14-00017601, https://apps.fcc.gov/edocs_public/attachmatch/DA-16-242A1.pdf (describing Verizon's injection of unique tracking IDs into mobile users' web browsing traffic).

[11] See Ryan Gallagher, Operation Socialist: The Inside Story of How British Spies Hacked Belgium's Largest Telco, The Intercept, December 13, 2014, https://theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story/. See also Andy Müller-Maguhn *et al.*, Map Of The Stars: The NSA and GCHQ Campaign Against German Satellite Companies, The Intercept, September 14, 2014, https://theintercept.com/2014/09/14/nsa-stellar/.

[12] *See* Kate Murphy, New Hacking Tools Pose Bigger Threats to Wi-Fi Users, New York Times, February 16, 2011, http://www.nytimes.com/2011/02/17/technology/personaltech/17basics.html.

websites. This encryption technology, known as HTTPS, is displayed to the user as a lock icon in a web browser.

17. Encryption typically provides three security benefits: Confidentiality, Integrity and Authentication. What this means is that when a software client (such as a web browser) uses encryption to protect data that is transmitted to a server (such as a web site), encryption protects that data from interception by third parties (confidentiality), it ensures that the client and server will know if a third party has tampered with the data as it is transmitted between them (integrity), and can permit the client and server to be confident that they are talking to each other and not an imposter (authentication).

18. In his declaration, Special Agent Alfin confirms that the NIT used by the FBI in the Playpen operation did not use an encrypted connection to transmit data from the target computers back to the FBI server.[13]

19. Because the FBI's NIT did not use encryption, the data that was transmitted by the NIT to the FBI's server was vulnerable to both interception and tampering by third parties as it was transmitted over the Internet.

20. That the FBI did not use encryption to protect data transmitted between the NIT and the FBI's server is in direct conflict with industry cybersecurity best practices and US government policy.[14]

21. Senior federal officials including the FBI Director have, for nearly half a decade, stressed the importance of using encryption to protect data that is transmitted over the internet.[15]

---

[13] *See* Alfin Declaration, paragraph 28, page 6.

[14] *See* Tony Scott, Policy to Require Secure Connections across Federal Websites and Web Services, infra fn X.

[15] *See* Pamela Jones Harbour, Remarks Before Third FTC Exploring Privacy Roundtable Washington, D.C, March 17, 2010, https://www.ftc.gov/sites/default/files/documents/public_statements/remarks-third-federal-trade-commission-exploring-privacy-roundtable/100317privacyroundtable.pdf ("[Security needs to be a default in the cloud. Today, I challenge all of the companies that are not yet using [HTTPS] by default. That includes all email providers, social networking sites, and any website that transmits consumer data. Step up and protect consumers. Don't do it just some of the time. Make your websites secure by default.") See also Lance Whitney, Senator wants more secure Web sites for Wi-Fi use, CNET News, February 28, 2011, https://www.cnet.com/news/senator-wants-more-secure-web-sites-for-wi-fi-use/. *See also* James B. Comey, Statement Before the House Judiciary Committee Washington, D.C. March 01, 2016, https://www.fbi.gov/news/testimony/encryption-tightrope-balancing-americans-security-and-privacy https://www.fbi.gov/news/testimony/encryption-tightrope-balancing-americans-security-and-privacy (Encryption is a "key tool to secure commerce and trade, safeguard private information ... and strengthen cyber security").

22. In 2015, the White House announced a new Office of Management and Budget policy requiring all federal agencies to encrypt their websites by the end of 2016.[16] Both the FBI and DOJ websites have since enabled encryption by default.

23. As the FBI did not use encryption to protect the connection between the NIT and the FBI's server, the agency has no way to be sure that the data collected by the NIT was not tampered with by third parties as it was transmitted over the internet to the FBI's server.

24. The integrity protection provided by encryption can be thought of as similar to the role of a tamper-evident seal in an evidence bag used by law enforcement. The digital evidence bag that the FBI used to transmit NIT data was neither signed nor sealed, and the FBI has no way of knowing what happened to the evidence before it reached the FBI's server.

The Network Data Stream

25. The government has offered to permit the defense to examine a copy of the "two-way network data stream", which Special Agent Alfin states "reflect[s] the information transmitted to the FBI from ███'s computer."[17] Special Agent Alfin's description is incorrect. As the network data stream was recorded at an FBI facility, the stream reflects the information received by the FBI, not the information transmitted by the NIT. As the NIT did not use an encrypted connection, the data sent by the NIT may have been modified in transit, and as a result, the data received by the FBI may be different than the data transmitted by the NIT.

26. The network data stream is not evidence of a chain of custody of the data transmitted by the NIT, nor would examining it reveal if any of the data transmitted by the NIT was tampered with as it was transmitted over the Internet to the FBI's server.

27. The network data stream is akin to a video recording of a forensic scientist at a FBI crime lab opening up an evidence bag and testing the evidence inside. However, if the bag was

---

[16] *See* Tony Scott, HTTPS-Everywhere for Government, White House Blog, June 8, 2015, https://www.whitehouse.gov/blog/2015/06/08/https-everywhere-government. *See also* Tony Scott, Policy to Require Secure Connections across Federal Websites and Web Services, Memorandum For the Heads of executive departments and agencies, Office of Management and Budget, June 8, 2015, https://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-13.pdf.
[17] *See* Alfin Declaration, paragraph 16, page 3.

6

not sealed, the video footage can only show that the evidence was appropriately handled once it was received by the crime lab, not what may have happened to the evidence between the time when it was placed in the evidence bag and the time that it was received by the crime lab.

28.   In his declaration, Special Agent Alfin states that the fact that the FBI's NIT did not use an encrypted connection is actually a good thing, as it enabled the FBI to capture a copy of the network data stream:

> "In fact, the network data stream that has been made available for defense review would be of no evidentiary value had it been transmitted in an encrypted format. Because the data is not encrypted, ▇▇▇ can analyze the data stream and confirm that the data collected by the government is within the scope of the search warrant that authorized the use of the NIT. Had the data been transmitted in an encrypted format the data stream would be of no evidentiary value as it could not be analyzed."[18]

29.   Special Agent Alfin's statement is incorrect. The FBI could have encrypted the connection between the NIT and the FBI's server, while also being able to capture a forensically valid copy of the network data stream.[19]

The Importance of the Exploit Code

30.   Engineers routinely make mistakes when designing software and inadvertently introduce software flaws into the code they write. These flaws can, in some cases, be exploited by third parties to gain or exceed authorized access to a computer without the knowledge or consent of the user.

31.   It is extremely difficult to write software without exploitable security flaws. Large, respected software companies like Google and Microsoft employ hundreds of engineers focused on computer security yet exploitable security flaws are regularly found in their products.

---

[18] *See* Alfin Declaration, paragraph 28, page 6.
[19] For example, the FBI could have used a termination proxy, so that the connection between the NIT and the FBI's network would be encrypted, after which, the data could flow unencrypted over the FBI's internal network to the NIT server. The network data stream could be captured either on the NIT server itself, or from another device inside the FBI's network.

7

32.   Security researchers regularly discover software security flaws in all kinds of software, including web browsers, word processing programs, operating systems, and even government-grade malware. For example, in 2011, computer security experts discovered exploitable security flaws in surveillance software used by the German police that left systems that were being remotely monitored by the German authorities vulnerable to unauthorized access by third parties.[20]

33.   Although it is perhaps possible that the exploit and NIT software used by the FBI in this operation are free of any flaws, it is extremely unlikely. Moreover, that the NIT did not use an encrypted connection to transmit data back to the FBI raises serious questions about what other cybersecurity best practices may have been ignored by the government contractors who wrote the exploit and NIT code for the FBI.

34.   Special Agent Alfin states in his declaration that while "it is theoretically possible for an exploit to make fundamental changes or alterations to a computer system … the NIT used here and the exploit used to deliver it did not."[21] Even if the FBI did not *intend* to make any permanent modifications to the computers targeted in the Playpen investigation or leave those systems open to compromise by third parties, it is possible that design flaws in the FBI's software may have inadvertently modified the defendant's computer system or otherwise left it in a vulnerable state. To determine what, if any, modifications were made to the defendant's computer system and the state in which it was likely left by the FBI, the defense must be able to examine all of the FBI code that the defendant's computer executed (that is, both the exploit code and the NIT).

   DONE this 10th day of June, 2016.

Christopher Soghoian
_____
Christopher Soghoian

---

[20] *See* Chaos Computer Club analyzes government malware, October 8, 2011,
http://ccc.de/en/updates/2011/staatstrojaner.
[21] *See* Alfin Declaration, paragraph 14, page 3.

8

FEDERAL PUBLIC DEFENDER
EASTERN DISTRICT OF VIRGINIA
150 BOUSH STREET, SUITE 403
NORFOLK, VIRGINIA 23510
TEL: (757) 457-0860
FAX: (757) 457-0880
Email: Amanda_Conner@fd.org

Geremy C. Kamens
Federal Public Defender

Amanda Conner
Assistant Federal Public Defender

July 29, 2016

<u>VIA EMAIL</u>
Elizabeth Yusi
United States Attorney's Office
101 West Main Street, Suite 8000
Norfolk, VA 23510
Email: Elizabeth.Yusi@usdoj.gov

RE: *U.S. v.* ███████████, Crim. No. 2:16cr92 – Discovery

Dear Beth:

I write to request additional discovery in the above-reference case. We request all information[1] related to the Playpen investigation. Specifically, we request all information related to the contents of the Playpen "main page"[2] at the time that the network investigative technique (NIT) was deployed against ███████████'s computer, which appears to have been in or around February or March 2015. This request includes all information related to changes to the main page, specifically information relevant to whether—at the time the NIT was deployed against ███████████'s computer—the main page contained two images depicting partially clothed prepubescent females with their legs spread apart. This request also includes information relevant to when the contents of the main page changed, who made the change, and when law enforcement learned of any change.

Second, we request all information demonstrating the number of new members who joined Playpen after February 20, 2015.

Third, we request all information demonstrating how many users visited Website A during the period that the FBI operated it.

Fourth, we request all information demonstrating how many users visited Website A on a weekly basis before the FBI took over the site.

Fifth, we request copies of the source code for all software that the government used to identify ███████████ including the payload or "NIT"; the exploit; the "unique identifier" generator; and the server software.

Sixth, we request copies of any and all memoranda, notes, emails, or other documents in which members of the investigative team discussed how the NIT warrant affidavit was to be

---
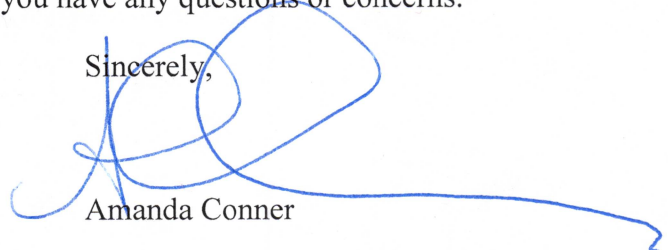
[1] The term "information" is meant to encompass all documents and other material that is subject to discovery under Rule 16 and/or the agreed discovery order entered in this case, as well as *Brady* material.
[2] The affidavit by Douglas Macfarlane in support of the application for a NIT warrant refers to the "main page" of Website A. Website A is "Playpen."

119

phrased, including any discussion of whether the warrant would state on its face that searches were to be conducted only in the Eastern District of Virginia. We also request any materials in which members of the Department of Justice or the FBI discussed the legal authority for issuance of a NIT warrant that purported to authorize the searches of places located outside the district in which the authorizing magistrate sat.

Please do not hesitate to contact me if you have any questions or concerns.

Sincerely,

Amanda Conner

2

JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA,	)	No. CR16-5110RJB
Plaintiff,	)))	**MOTION AND MEMORANDUM IN SUPPORT OF MOTION TO COMPEL DISCOVERY**
v.	))	
████████████,	))	*[Oral Argument Requested]*
	)	**NOTED: September 30, 2016**
Defendant.	))	

UNITED STATES OF AMERICA,	)	No. CR15-387RJB
Plaintiff,	)))	**MOTION AND MEMORANDUM IN SUPPORT OF MOTION TO COMPEL DISCOVERY**
v.	))	
████████████,	))	*[Oral Argument Requested]*
Defendant.	))	**NOTED: September 30, 2016**
	)	

UNITED STATES OF AMERICA,	)	No. CR15-274RJB
Plaintiff,	)))	**MOTION AND MEMORANDUM IN SUPPORT OF MOTION TO COMPEL DISCOVERY**
v.	))	
████████████,	))	*[Oral Argument Requested]*
Defendant.	))	**NOTED: September 30, 2016**
	)	

I. INTRODUCTION

Defendants ███████████████████ and ███████████, through their attorneys, respectfully move the Court pursuant to Fed. R. Crim. P. 16(d) for an Order compelling discovery material to their pending Motions to Dismiss the Indictment (dkt. 32) and Motions to Suppress (dkt. 35). This motion is supported by the following memorandum of law, as well as the accompanying certification of defense counsel in compliance with Local Rule CrR 16(i).

The trials are now scheduled for January 23, 2017, with a new pretrial motion deadline of December 16, 2016.

II. BACKGROUND AND FACTS

On September 12 and 20, 2016, the parties requested the following discovery from the Government:

1. All records related to the Government's review and approval of Operation Pacifier.

The defense has offered to examine these particular records pursuant to a protective order limiting review to defense counsel and the Court.

The Department of Justice's internal procedures and guidelines require a special review and approval process for undercover online investigations. Discovery of the records related to this process will likely confirm the Government's knowledge that it was not authorized to seek worldwide NIT warrants, an issue directly relevant to the defendants' Motion to Suppress and any claim by the Government that it acted in "good faith." In addition, the process leading to the Government's decision to ignore the law prohibiting distribution of child pornography from the Playpen site is relevant to the defendants' pending Motions to Dismiss the Indictment based on outrageous conduct.

2. Copies of any reports made to the National Center for Missing and Exploited Children (NCMEC) regarding child pornography posted on the Playpen web site.

3. Copies of any notifications that were sent to victims by the Government for obtaining restitution related to images that were posted on, or distributed from, the Playpen web site.

Items 2 and 3 also relate to the Motion to Dismiss, since they are likely to yield additional evidence that the FBI made no effort to track or contain the child pornography that was posted on its site and that it has made little or no effort to meet its victim notification and restitution obligations. This information is also relevant to any restitution claims the Government may seek to level against the defendants, in terms of the Government's potential joint liability for restitution and the equities of any restitution amounts claimed by the Government.

4. The number of new images and videos (*i.e.* content not previously identified by NCMEC) that was posted on the site between February 20, 2015 and March 5, 2015.

Item 4 is likely to reveal evidence that the FBI's operation of Playpen resulted in the posting and distribution of new child pornography, a particularly egregious consequence of its decision to keep the site not only fully functional but also encourage and increase visitor traffic to Playpen.

5. The names of all agents, contractors or other personnel who assisted with relocating, maintaining and operating Playpen while it was under Government control.

6. Copies of all notes, emails, reports, postings, etc. related to the maintenance, administration and operation of Playpen between February 20, 2015 and March 5, 2015.

Items 5 and 6 are needed by the defense to identify potential witnesses for an evidentiary hearing (if granted) on the FBI's operation of Playpen. Further, this discovery relates to the FBI's efforts to improve and expand the site's distribution capabilities, an issue material to the pending outrageous governmental conduct issues. *See* dkt. 32 and exh. A, attached hereto (copy of dkt. 40, evidencing the FBI's efforts to improve Playpen's performance and attract new postings).

7. Copies of all legal memoranda, emails and other documents related to the legality of the FBI's operation of Playpen (and the distribution of child pornography by the Government), including requests for agency/departmental approvals of the undercover operation of Playpen and any communications with "Main Justice" or the Office of General Counsel at the FBI.

This discovery request is material to further establishing that the Government's violation of Fed. R. Crim. P. 41 was deliberate and, consequently, requiring suppression under *United States v. Weiland*, 420 F.3d 1062 (9th Cir 2005)).

This request is also material to rebutting any claim by the Government that the Court should excuse its jurisdictional and Fourth Amendment violations under the "good faith" exception to the exclusionary rule. *See, e.g., United States v. Croghan*, 2016 WL 4992105 at * 8 (D. Iowa Sept. 19, 2016) (suppressing all fruits of an NIT search and finding that "law enforcement was sufficiently experienced, and that there existed adequate case law casting doubt on magisterial authority to issue precisely this type of NIT Warrant, that the good faith exception is inapplicable.").

8. Copies of all correspondence, referrals and other records indicating whether the exploit used in the Playpen operation has been submitted by the FBI or any other agency to the White House's Vulnerability Equities Process (VEP) and what, if any, decision was made by the VEP.

This request is material because federal agencies are required to submit information about computer security vulnerabilities and the use of malware for investigatory purposes for VEP review and approval to ensure that use of the malware complies with all applicable laws and does not pose substantial risks to the public. *See generally* Electronic Privacy Information Center, *Vulnerability Equities Process,* available at: https://epic.org/privacy/cybersecurity/vep/default.html; *see also United States v. Michaud*, CR15-05351RJB, dkt. 195 (Mozilla's Motion to Intervene) ("The

124

information contained in the Declaration[s] of Special Agent Alfin suggests that the Government exploited the very type of vulnerability that would allow third parties to obtain total control an unsuspecting user's computer.")

9. Copies of invoices and other documents for the hosting facility/facilities where the Government operated the Playpen server, the server from which the Government delivered the NIT malware and the server that NIT targets sent their identifying information back to, including documents revealing whether the Government informed the hosting provider(s) that child pornography would be stored in their facility or transmitted over their networks.

This discovery is also material to the pending Motion to Dismiss and to rebut a claim of "good faith," because it is likely to further establish that the FBI violated the law by distributing child pornography and reveal the full extent of this illegality, including the FBI's failure to notify innocent third parties and Internet service providers that they were being placed in possession of contraband or helping to distribute it.

10. The number of Playpen-related investigations that have been initiated but did not result in criminal charges, beyond the approximately 200 cases now pending across the country.

11. The total number of IP addresses and MAC IDs that were seized during the time the FBI was operating Playpen, over and above those related to these approximately 200 pending cases.

Items 9 and 10 are material to the defendants' pending Motions to Suppress, in particular to help establish that the FBI misrepresented in the NIT warrant application the likelihood that visitors to Playpen were intentionally seeking to download or distribute child pornography and the ability of the NIT to accurately identify legitimate targets.

125

12. The number of IP addresses and MAC IDs obtained during the investigation from foreign computers and the countries in which this data was obtained.

This final category of information is relevant to determining the extent to which the FBI violated foreign law and U.S. treaty obligations by deploying malware and distributing child pornography overseas. This information also is relevant to determining the legality of the NIT warrant itself, which appears to have been issued in violation of foreign laws and United States's international legal obligations.

The Government has declined to provide any of the requested information.

III.   UNDER THE CONTROLLING NINTH CIRCUIT LAW, THE DEFENSE IS ENTITLED TO THIS DISCOVERY.

On September 16, 2016, the Ninth Circuit issued a new opinion on the scope of discovery required under Fed. R. Crim. P. 16 and that decision supports disclosure of the records and information sought by this motion. In *United States v. Soto-Zuniga*, 2016 WL 4932319 (9th Cir. Sept. 16, 2016), the Court of Appeals reversed the defendant's conviction for drug trafficking because the district court had abused its discretion by failing to order discovery of records and reports that were material to potential pre-trial motions and defenses at trial.

The defendant in *Soto-Zuniga* was arrested and charged after the police stopped his car at an immigration check point and found drugs. *Id*. at * 2. The defense wanted to determine whether the police had complied with the requirements for a constitutionally permissible check point by reviewing the check point's stop and arrest statistics. *Id*. at * 5. The defendant also sought law enforcement records related to several third parties who may have been responsible for placing drugs in his vehicle. *Id*. at * 8. The district court denied these discovery requests, finding that they were unlikely to lead to admissible evidence and that granting the requests would needlessly prolong the case. *Id*. at * 7.

126

The Ninth Circuit reversed and remanded with instructions to grant the defendant's discovery motions. The court also ordered the trial court to allow the Government "a window of time" to propose protective measures for any sensitive information and to determine whether it would prefer to dismiss the case rather than comply with the disclosure order. *Id.* at * 8.

In reaching this conclusion, the court emphasized that defendants have a right to all discovery that is "material to preparing the defense" under Fed. R. Crim. P 16. *Id.* 16(a)(1)(E).

Further, "[m]ateriality is a 'low threshold; it is satisfied so long as the information. . .would have helped to prepare a defense." *Id.*, citing *United States v. Hernandez-Meza*, 720 F.3d 760, 768 (9th Cir. 2013). The court also explained that it does not matter whether the discovery consists of evidence that would be admissible at trial. All the defense need show is that it may assist in developing pre-trial motions or lead to admissible evidence. *Id.* Indeed, as this Court has also recognized, discovery "is material even if it simply causes a defendant to completely abandon a planned defense and take an entirely different path." *Id.*

Given this law, and the relevance of the discovery sought in this case, the defendants respectfully request that the Court order the Government to provide that discovery.

The defense has no objection to the Court's issuance of an appropriate protective order for any discovery for which it finds that the Government has legitimate concerns about public disclosure or to address any legitimate claims of privilege.

///

///

///

///

127

IV. CONCLUSION

For the reasons stated above, the Court should grant the Motion to Compel

Discovery.

DATED this 22nd day of September, 2016.

Respectfully submitted,

s/ *Colin Fieman*
Attorney for ███████

s/ *Robert Goldsmith*
Attorney for ███████

s/ *Mohammad Hamoudi*
Attorney for ███████

███

128

CERTIFICATE OF SERVICE

I hereby certify that on September 22, 2016, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to all parties registered with the CM/ECF system.

s/ *Amy Strickling, Paralegal*
Federal Public Defender Office

JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA,	)	No. CR15-5351RJB
Plaintiff,	)))	MOTION AND MEMORANDUM OF LAW IN SUPPORT OF MOTION TO
v.	))	COMPEL DISCOVERY
███████████,	))	**Noted: December 4, 2015**
Defendant.	)))	*[Evidentiary Hearing Requested]*

I. MOTION

████████ by his attorneys Colin Fieman and Linda Sullivan, respectfully moves the Court pursuant to Fed. R. Crim. P. 16(d) for an Order compelling discovery material to the defense's pending Motion to Suppress and Motion to Dismiss Indictment. This motion is supported by the following memorandum of law and attached exhibit, as well as the accompanying certification of defense counsel in compliance with Local Rule CrR 16(i).

II. FACTS AND ARGUMENT

On September 9, 2015, the defense requested a copy of the programming code for the "Network Investigative Technique" (NIT) that was deployed on ████████'s computer. The defense is seeking a copy of the code so that its computer forensics expert can independently determine the full extent of the information the Government seized from ████████'s computer when it deployed the NIT; whether the NIT

interfered with or compromised any data or computer functions; and whether the Government's representations about how the NIT works in its warrant applications were complete and accurate. This forensic information is relevant to ███████'s Motion to Suppress and a potential motion pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). *See United States v. Cedano-Arellano*, 332 F.3d 568 (9th Cir. 2003) (district court erred in denying a defendant's motion for discovery under Rule 16 of material relating to the reliability of a drug-sniffing dog, for purposes of a motion to suppress); *United States v. Gamez-Orduno*, 235 F.3d 453, 462 (9th Cir. 2000) (requiring disclosure on due process grounds of a report relevant to issues in a suppression motion); *see also* W.D.. Wa. Local Rule CrR 16 ("It is the intent of the court to encourage complete and open discovery consistent with applicable statutes, case law, and rules of the court at the earliest practicable time").

The defense has offered to enter into a protective order that would ensure that review of the programming code is limited to the defense team and also address any other legitimate confidentiality concerns the Government may have about disclosing the code. However, on October 30, 2015, the Government notified the defense that it would not disclose the code, asserting that it is "subject to law enforcement privilege."

The Court should note that, in connection with other NIT cases, the Government has made copies of the NIT's programming code available to the defense for inspection and forensic analysis. *See* Motion to Vacate Protective Order, exh. A at 2 (Department of Justice (DOJ) notice and disclosure letter in *United States v. Cottom*, summarizing the Government's disclosures about the NIT "Flash application" used in that case, including "example programming code," and extending an offer for defense inspection of the "compiled code for the NIT" stored on a government server). The Government's

refusal to disclose the code in this case is therefore inconsistent with its prior practice and in itself cause for concern.

In addition, the defense served the Government with a supplemental discovery letter on October 22, 2015, seeking information relevant to ███████████'s Motion to Dismiss Indictment. *See* exh. A, attached hereto (discovery request letter). The requested information includes the total number of pictures and videos that were downloaded or distributed from "Website A" while it was managed and controlled by the FBI; the number of visitors to the site during that time; and records related to the approval and supervision of the "Website A" operation.

The Government has not disputed that it can access and provide all of the data and records identified in the October 22 request. However, it has declined to disclose the information requested on several grounds, including relevance and "law enforcement privilege."[1]

All of the information sought by the defense in its October 22 request relates to the allegations of outrageous governmental conduct that are the subject of the dismissal motion. This information is relevant to showing the extent to which the Government distributed child pornography during the FBI's control and administration of "Website A" and the defense's ability to meet its burden of showing that the Government's conduct offends common standards of decency to a degree warranting dismissal. Likewise, the request for documents and records relating to DOJ's review, approval and supervision of the "Website A" operation are relevant to showing that the FBI's distribution of child pornography as part of that operation was not a mistake or undertaken by agents acting without FBI or DOJ approval, and was in fact a course of action approved by the Government.

---

[1] The Government has made available an "offline copy" of "Website A" for defense inspection, but the data relating to the discovery request cannot be gleaned from this copy.

Finally, the discovery related to DOJ's and the FBI's approval and supervision of the "Website A" operation is also relevant to rebutting specific claims the Government has made in its Response to Motion to Suppress (Dkt. 47). There, in arguing that agents acted in "good faith" reliance on the NIT warrant, the Government has contended that agents "deliberately sought to satisfy the letter of Rule 41" and that "law enforcement" concluded that the NIT warrant application complied with the law. *Id.* at 21. Although the subjective beliefs and intentions of law enforcement agents are irrelevant for purposes of the good faith exception, *see, e.g, United States v. Hove*, 848 F.2d 137, 140 (9th Cir. 1988), the Government is nonetheless suggesting that the Court should consider facts related to DOJ's internal review or approval of the "Website A" warrants when deciding whether the good faith exception should apply. Having raised these factual issues, the Government should not be allowed to withhold discovery that sheds further light on them.[2]

III. CONCLUSION

For the reasons stated above, █████████ respectfully requests that the Court issue an Order for disclosure of the records and information sought by the defense, subject to such conditions or protections that the Court deems appropriate to address any legitimate confidentiality interests on the part of the Government.

DATED this 20th day of November, 2015.

Respectfully submitted,

s/ *Colin Fieman*
s/ *Linda Sullivan*
Attorneys for █████████

---

[2]The Government's response to the motion to suppress, including its good faith argument, will be addressed fully in the defense's suppression motion reply briefing, which is due on December 2, 2015.

CERTIFICATE OF SERVICE

I hereby certify that on the date shown below I e-filed with the Clerk of the Court the foregoing Motion to Compel Discovery and Memorandum in Support of Motion, Proposed Order, and Affidavit and Certification of Defense Counsel in Support of Motion to Compel Discovery. I used the CM/ECF system, which will send notification of this filing to Special Assistant United States Attorney.

DATED this 20th day of November, 2015.

s/ Amy Strickling, Paralegal to
Colin Fieman
Assistant Federal Public Defender

FEDERAL PUBLIC DEFENDER
Western District of Washington

October 22, 2015

<u>Via email & mail</u>

Kate Vaughan
Assistant United States Attorney
700 Stewart Street - Suite 5220
Seattle, WA 98101-1271

      Re: *United States v.* ▉▉▉▉ CR15-5351

Dear Ms. Vaughan,

      Thank you for your email of October 21, confirming that "Website A" users were able to access child pornography (CP) while the site was under the administrative control of the FBI. Given this information, we request the following additional discovery:

- The number of CP pictures that were posted on the site between February 20 and March 4, 2015;

- The number of CP videos that were posted on the site during that time period;

- The number of links to CP pictures and videos that were posted on the site during that time period;

- The number of CP pictures that were viewed and the number of CP videos that were viewed during that time period.

- The number of CP pictures that were downloaded and the number of CP videos that were downloaded during that time period.

- The number of visitors to the site between February 20 and March 4, 2015, and the number of total visits (recognizing that distinct visitors may have visited the site more than once).

- Some measure of the length of the visits (e.g., total time all visitors were connected to the site; average time visitors were connected to the site).

Kate Vaughan
October 22, 2015
Page 2

- A summary of any measures that were taken by the FBI or other law enforcement entities to block access to the pictures, videos and links available on or through the site between February 20 and March 4, 2015;

- The reason the site was shut down on March 4 (rather than earlier or later); and

- All documents relating to review and authorization of the FBI's administrative control of the site by the Department of Justice or other governmental agencies that were involved in the "Website A" investigation and deployment of the NIT at issue in our case.

I realize that coming up with exact picture, video and link totals may be time consuming, but if you can provide at least a good faith estimate of the numbers at this time, we can request more specific information later if needed.

Thank you for your cooperation.

Sincerely,

Colin Fieman
Assistant Federal Public Defender

cf

EXHIBIT A-002

JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA,	)	No. CR15-5351RJB
	)	
Plaintiff,	)	THIRD MOTION AND
	)	MEMORANDUM OF LAW IN
v.	)	SUPPORT OF MOTION TO COMPEL
	)	DISCOVERY **[FILED UNDER SEAL]**
███████████,	)	*[Evidentiary Hearing Requested]*
	)	
Defendant.	)	**Noted: January 22, 2016**
	)	

I. MOTION

████████ by his attorneys Colin Fieman and Linda Sullivan, respectfully moves the Court pursuant to Fed. R. Crim. P. 16(d) for an Order compelling discovery relevant to the defense's pending Motions to Suppress, *Franks* Motion, and ███ █████'s defense at trial. This motion is supported by the following memorandum of law and attached exhibits, as well as the accompanying certification of defense counsel in compliance with Local Rule CrR 16(i).

For the reasons discussed below, the defense further requests that the Court schedule an expedited hearing on this motion.

II. FACTS AND ARGUMENT

On September 9, 2015, the defense asked the Government to provide a copy of the programming code for the "Network Investigative Technique" (NIT) that was

deployed on a computer that ███████ allegedly possessed. The Government declined to produce the code.

On November 20, 2015, the defense filed its First Motion to Compel Discovery. (Dkt. 54). As set forth in that motion, the defense was seeking, *inter alia*, a complete copy of the code so that a forensic expert can independently determine the full extent of the information the Government seized from ███████'s computer when it deployed the NIT; whether the NIT interfered with or compromised any data or computer functions; and whether the Government's representations about how the NIT works in its warrant applications were complete and accurate. (Dkt. 54).

In addition, as explained in the attached declaration of Vlad Tsyrkevich, the complete NIT code is necessary to establish the electronic "chain of custody" for the data that allegedly links a computer purportedly used by ███████ to activities on "Website A." *See* exh. A, attached hereto.

The Court scheduled a hearing on the first discovery motion for December 14, 2015.

On December 4, 2015, the Government filed a brief in opposition of discovery. (Dkt. 74). In that brief, the Government argued that the code was subject to a "qualified law enforcement privilege" and that its disclosure would compromise pending investigations and be "harmful to the public interest." *Id.* at 15.

On December 10, 2015, the Government notified the defense that it was withdrawing its objection to disclosing the NIT code. This agreement was memorialized on the record at the December 14 hearing. *See* Exh. B (December 14, 2015, Hearing Transcript) at 2. Further, the Government stated that it would seek to complete discovery by "the first week of January." *Id*. at 36.

On January 5, 2016, the Government filed a Stipulated Motion for Entry of Discovery Protective Order (Dkt. 96). The motion set forth the additional security measures the parties had agreed to for ensuring that the NIT data remained secure and confidential. The Court issued its NIT data protective order the same day. (Dkt. 102).[1]

On January 11, 2016, the defense's code expert, Vlad Tsyrkevich received a password protected disc from the FBI ostensibly containing the NIT data that the defense had requested.

Mr. Tsyrklevich made a preliminary assessment of the data on January 12 and then notified defense counsel that the data was incomplete. The same day, defense counsel emailed the Government and identified the missing information. The Government has declined to provide the missing NIT data, and this motion now follows.

III. ARGUMENT

As set forth in ▮▮▮▮▮▮▮'s November 20, 2015, Motion to Compel Discovery (Dkt. 54), a complete and accurate copy of the NIT code is relevant to the pending suppression motions, the motion to dismiss the indictment and, now, the motion

---

[1] The Government had originally wanted the defense to conduct its code analysis at an FBI facility. Defense counsel informed the Government that, according to one of the experts that the defense was considering retaining, this arrangement would be problematic because of the amount of time needed for analysis and the need to keep defense work product confidential. The Government then agreed to provide the data on a disc, with such security precautions as hand-to-hand delivery and return of the disc and password protections. It is important to note that the Government has never indicated that discovery of the NIT code was contingent on it being analyzed at a government facility. Nor did the Government ever inform the defense that it would be receiving less than the complete code after having reached an agreement about the appropriate security measures.

The defense has since retained a different expert, Vlad Tsyrklevich, in part because he has previously worked as a contractor for law enforcement and intelligence agencies and has had "top secret" clearance that would further assure the Government that the data would be handled properly. Mr. Tysrklevich is willing to analyze the missing code components at a government facility in New York City (where he is located) if necessary.

pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978). *See United States v. Cedano-Arellano*, 332 F.3d 568 (9th Cir. 2003) (district court erred in denying a defendant's motion for discovery under Rule 16 of material relating to the reliability of a drug-sniffing dog, for purposes of a motion to suppress); *United States v. Gamez-Orduno*, 235 F.3d 453, 462 (9th Cir. 2000) (requiring disclosure on due process grounds of a report relevant to issues in a suppression motion); *see also* W.D. Wa. Local Rule CrR 16 ("It is the intent of the court to encourage complete and open discovery consistent with applicable statutes, case law, and rules of the court at the earliest practicable time").

Further, defense analysis of the code is not only relevant to ▮▮▮▮▮▮▮'s defense at trial, but necessary to verifying the "chain of custody" for the data that the Government alleges links a computer attributed to ▮▮▮▮▮ to activities on "Website A." *See* exh. A (Tsyrkevich Declaration) at ¶ 6; *see also*, *e.g.*, *United States v. McDuffie*, 454 F. App'x 624, 626 (9th Cir. 2011) (affirming grant of new trial based on Government's late disclosure of evidence that detective's fingerprint was on drug scale; court noted that the late disclosure prevented, *inter alia*, defendant from conducting "any pre-trial discovery into the scale's chain of custody"); *United States v. Brewster*, 2009 WL 804709, at *4 (D. Idaho Mar. 27, 2009) (concluding that, because Government has stated it has "abide[d] by its duties under Rule 16 . . . any relevant records to chain of custody would have been provided to Defendant"); *United States v. W.R. Grace*, 233 F.R.D. 586, 590 (D. Mont. 2005) (ordering, pursuant to Rule 16(a)(1)(E)(i) [items material to the defense] "All documents relating to the chain of custody for" [asbestos samples]).

The Government's failure to provide complete NIT code to the defense is a matter of some urgency. The Court has scheduled a hearing on the pending suppression

and *Franks* motions for January 22, the deadline for all pre-trial motions is January 28, and ███████'s February trial date is rapidly approaching. Accordingly, the defense requests that the Court set an expedited schedule for responsive briefing by the Government and also schedule a hearing on this motion for Tuesday, January 19, 2016, if the Court's docket allows.

IV. CONCLUSION

For the reasons stated above, ███████ respectfully requests that the Court issue an Order for disclosure by the Government of the complete NIT code data, as well as any related records or information that are needed for the defense's analysis of that data.

DATED this 14th day of January, 2016.

Respectfully submitted,

s/ *Colin Fieman*
s/ *Linda Sullivan*
Attorneys for ███████

CERTIFICATE OF SERVICE

I hereby certify that on the date shown below I e-filed with the Clerk of the Court the foregoing Third Motion to Compel Discovery and Memorandum in Support of Motion **[FILED UNDER SEAL]**, Proposed Order, and Certification of Defense Counsel in Support of Third Motion to Compel Discovery. I used the CM/ECF system, which will send notification of this filing to Special Assistant United States Attorney.

I further certify that I delivered a copy of the above sealed documents to the registered parties via email.

DATED this 14th day of January, 2016.

s/ Amy Strickling, Paralegal to
Colin Fieman
Assistant Federal Public Defender

JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA,	)	No. CR15-5351RJB
Plaintiff,	)	
	)	
v.	)	DECLARATION OF VLAD TSYRKLEVICH
	)	
███████████,	)	
	)	
Defendant.	)	
	)	

I, Vlad Tsyrklevich, declare under penalty of perjury that:

1.   I have been retained by ████████'s defense team to conduct a forensic analysis of the "Network Investigative Technique" (NIT) that was used to search for and seize data in this case. A copy of my *curriculum vitae* is attached to this declaration.

2.   On January 11, 2016, I received a password protected disc from the FBI which, according to the information I had been provided by defense counsel, would contain the programming (or "source") code for the investigative technique. Prior to receiving this disc, I had reviewed and agree to abide by the terms of a confidentiality agreement and protective order that had been drafted by the government.

3.   After conducting an initial examination of the code that had been provided by the FBI it was apparent that to me that the code was incomplete. A brief

DECLARATION OF VLAD TSYRKLEVICH
(*United States v* ████ *CR15-5351RJB)* - 1

143

A-001

1 explanation of how NITs work and their various components follows, along with an

2 explanation of the missing aspects of the code.

3   4. **The components of an NIT programming or source code and how they**

4 **work:** The NIT presented by the FBI works by using an "exploit," a piece of software

5 that takes advantage of a software "vulnerability" in the Tor Browser program. By

6 exploiting this software vulnerability, the NIT is able to circumvent the security

7 protections in the Tor Browser, which under normal circumstances, prevents web sites

8 from determining the true IP address or MAC address of visitors. After exploiting the

9 vulnerability, the NIT delivers a software "payload," a predetermined set of actions, to

10 computers that receive the payload (the "host computer"). The payload used by the FBI

11 in this case collected and then transmitted identifying information about the host

12 computer (including its IP address) along with a unique "identifier" used to associate

13 the target with the identifying information that the NIT collects. As a result, these type

14 of investigative techniques have four primary components:

15   a.   Software that generates a payload and injects a unique identifier

16   into it.

17   b.   The "exploit" that is sent to the target computer to take advantage
            of a software flaw in the Tor Browser.

18

19   c.   The "payload" that is run on the target computer to extract
            identifying information about it (such as its IP address).

20   d.   An additional "server component" that stores and preserves the

21   extracted information and allows investigators to access it.

22   5**.**   **What the FBI Produced and What is Still Missing:** The government

23 has provided us with one component of the payload (component "c"). However, it is

24 unclear from the limited data provided so far whether the payload that has been

25 provided was the only payload associated with the NIT or whether other payloads were

26 executed. Moreover, the FBI has not furnished component "a" (the server component

DECLARATION OF VLAD TSYRKLEVICH
(*United States v* ▮▮▮ *CR15-5351RJB*) - 2

144

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

A-002

that generates the payload and injects an identifier); "b" (the exploit component); or "d" (the data preservation component). It is all of these components in combination, not just one or another of them, that constitutes a network investigative technique.

6. **Why the Missing Components are Needed for a Complete and Accurate Analysis:** The accuracy and potential admissibility of the evidence collected by the NIT depends on the accuracy of the data the government claims is associated with the computer that ▮▮▮▮▮▮ allegedly used to access "Website A." In addition, defense counsel has informed me that he is seeking to determine if the NIT used in this case operated in the manner described in various warrant applications and whether its execution may have compromised any data or functions on the target computer. However, the materials provided by the FBI are insufficient to make these determinations or verify that the data extracted from the target computer is accurate for the following reasons:

- The software that generates a payload and injects a unique identifier into it (component "a") is critical to understanding whether the unique identifier used to link a defendant to access of illegal content is actually unique. If the identifier is generated incorrectly, it could cause different users to be incorrectly linked to each other's actions. It is important to note that errors in the use of cryptographic components are pervasive in modern software. The proper generation of unique identifiers hinges on the correct use of a "Pseudo-Random Number Generator," a fundamental cryptographic technology that is frequently misused. Without the missing data, I am unable to make a determination about these issues.

- As noted, the "exploit" used in the NIT (component "b") is intended to execute on the computer that is being identified. Analyzing and understanding the exploit component of the NIT is critical to understanding whether the payload data that has been provided in discovery was the only component executing and reporting information to the government or whether the exploit executed additional functions outside of the scope of the NIT warrant. Without the missing data about the exploit component of the NIT, I am unable to make a determination about these issues.

- In addition, the server component that stores the identifying information returned by the payload (component "d") must faithfully store and reproduce the data it was sent. The correct use of data storage primitives and the programming practices used to avoid data corruption or tampering make analyzing this

DECLARATION OF VLAD TSYRKLEVICH
(*United States v* ▮▮▮▮▮ *CR15-5351RJB*) - 3   145

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

A-003

1 component of the NIT essential to understanding and verifying the digital "chain
2 of custody" of information derived from the NIT. Without the missing data, I am
   unable to make a determination about these issues.

3   7.   The importance of this data to ███████████'s preparation of his defense is hard
4 to overstate because I am aware of a previous instance in which an NIT resulted in
5 indiscriminate targeting. In August 2013, all of the websites hosted by "Freedom
6 Hosting" -- a service, run from servers in France, that hosted websites accessible to
7 users of the Tor network -- began serving an error message with hidden code embedded
   in the page.[1] That code was specifically designed to exploit a security flaw in a version
8 of the Firefox web browser used to access Tor hidden servers.[2] According to an FBI
9 agent who later testified in an Irish court, the Freedom Hosting service hosted at least
10 100 child pornography websites.[3] But the service also hosted a number of legitimate
11 sites, including TorMail, a web-based email service that could only be accessed over
12 the Tor network, and the Hidden Wiki, which one news site described as the "de facto
13 encyclopedia of the Dark Net."[4] Even though these sites were serving lawful content,
14 the FBI's "watering hole" attack was performed in an overbroad manner, delivering a
15 NIT to visitors of all of the Freedom Hosting sites, not just to visitors of sites that were
16 engaged in the distribution of illegal content. It is therefore important to ███████████'s
17 defense and trial preparations to determine whether a similarly indiscriminate "watering
18 hole" attack could have affected this case.

19   DONE this 13th day of January, 2016.

21 _____
    Vlad Tsyklevich

23 _____

[1] *See* Kevin Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, Wired (Sept. 13, 2013),
24 http://www.wired.com/2013/09/freedom-hosting-fbi/.

[2] See Goodin, *Attackers Wield Firefox Exploit to Uncloak Anonymous Tor Users*, Ars Technica (Aug. 5, 2013),
25 http://arstechnica.com/security/2013/08/attackers-wield-firefox-exploit-to-uncloak-anonymous-tor-users/.

[3] Poulsen, *FBI Admits It Controlled Tor Servers Behind Mass Malware Attack*, *supra.*

26 [4] Patrick Howell O'Neill, *An In-Depth Guide to Freedom Hosting, the Engine of the Dark Net*, The Daily Dot
(Aug. 4, 2013), http://www.dailydot.com/news/eric-marques-tor-freedom-hosting-child-porn-arrest/.

DECLARATION OF VLAD TSYRKLEVICH
(*United States v* ████████ *CR15-5351RJB*) - 4   146

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

A-004

Vlad Tsyrklevich

(858) 722-6490

http://tsyrklevich.net

vlad@tsyrklevich.net

Skills

Languages: C, Ruby, Assembly (x86/x64, PPC, ARM, MIPS, SPARC), C++/Objective-C, Java, Python, JavaScript

Work Experience

- **Square** — San Francisco, CA and New York, NY
  Security Engineer — *04/2012 – Present*
  - Low-level iOS and Android platform analysis in order to develop custom security assurances and anti-RE measures
  - Develop a complex client-server software protection scheme integrating with an external hardware module
  - Audit services in production datacenters and work with the platform team to fix flaws and introduce new security measures
  - Consult with software engineering teams on secure application development, PKI, and network architecture

- **Irdeto** — San Francisco, CA
  Senior Reverse Engineer — *11/2011 – 04/2012*
  - Analyze and defeat custom protection schemes implemented in user- and kernel-land on Windows
  - Work with partners on hardening their copy-protection mechanisms against reverse engineering
  - Evaluate both in-house and third-party anti-RE solutions for use by our partners and in our software

- **SPARTA, Inc.** — Centreville, VA
  Security Researcher — *05/2006 – 11/2011*
  - Lead new research efforts in reverse engineering, vulnerability discovery and exploit development across Windows, Linux, and embedded platforms
  - Analyze undocumented network protocols and file formats in order to replicate behavior, bypass protection schemes and discover vulnerabilities
  - Reverse engineer armored and packed binaries and bypass anti-reverse engineering protection schemes
  - Develop low-level applications with high-speed, high-stealth and high-reliability considerations

Open Source

- **Metasploit Framework** — *2005 - 2006*
  - Develop payloads for Windows, Linux, Solaris and other operating systems across multiple architectures
  - Port public exploits and write new exploits, shellcode encoders, nop generators and backend plug-ins

Education

University of California, Berkeley
B.A. Applied Math with a focus in Computer Science; GPA: 3.6

Presentations

- Co-speaker at Blackhat USA 2007: Single Sign-On for the Internet: A Security Story

- Speaker at Toorcon San Diego 2006: Polymorphic Shellcode at a Glance

147

1

A-005

EXHIBIT TO FOURTH SAMPLE MOTION TO COMPEL

1   UNITED STATES DISTRICT COURT
           WESTERN DISTRICT OF WASHINGTON
2   AT TACOMA

3 .

4 UNITED STATES OF AMERICA,   )   Docket No. CR15-5351RJB
)
5   Plaintiff,   )   Tacoma, Washington
)
6 vs.   )   December 14, 2015
)
7 ███████████,   )
)
8   Defendant.   )
  _____)

9

10

11   TRANSCRIPT OF PROCEEDINGS
         BEFORE THE HONORABLE ROBERT J. BRYAN
         SENIOR UNITED STATES DISTRICT COURT JUDGE
12

APPEARANCES:
13
For the Plaintiff: KEITH BECKER
14   ANDRE PENALVER
                        U.S. Department of Justice
15   1400 New York Avenue NW, 6th Floor
                        Washington, DC 20530
16
For the Defendant: COLIN FIEMAN
17   LINDA SULLIVAN
                        Office of the Public Defender
18   1331 Broadway, Suite 400
                        Tacoma, Washington 98402
19
Court Reporter: Teri Hendrix
20   Union Station Courthouse, Rm 3130
                        1717 Pacific Avenue
21   Tacoma, Washington 98402
                        (253) 882-3831
22

23 Proceedings recorded by mechanical stenography, transcript
   produced by Reporter on computer.
24

25

1   Monday, December 14, 2015 - 10:30 a.m.

2   (Defendant present.)

3   THE CLERK: All rise. This United States District

4 Court is now in session, the Honorable Robert J. Bryan

5 presiding.

6   THE COURT: Please be seated.   Good morning.

7   This is United States versus ████████, No. 15-5351. It

8 comes on for argument today on the defendant's motion to

9 compel. The defendant is present with his attorneys,

10 Ms. Sullivan and Mr. Fieman. And is it Mr. Becker for the

11 government?

12   In preparation for this hearing, I have read the motion

13 and memorandum in support of the motion, and the government's

14 response and the defendant's reply. I have also looked at the

15 motion to dismiss the indictment, which was referenced in the

16 pleadings. So I think we are ready to proceed here.

17   Okay, Mr. Fieman, this is your motion, you may proceed.

18 It is my understanding that a good part of the original motion

19 has been resolved.

20   MR. FIEMAN: Yes, thank you, Your Honor.

21   As indicated in my responsive pleading, the government

22 notified us on Thursday that they were in fact willing to turn

23 over the NIT code, which we appreciate. That, I think,

24 resolves a significant portion of what we were prepared to

25 address today. And just to update the government as well, we

1   are in the process of retaining an expert on code analysis and

2   expect that that part of the discovery will proceed smoothly.

3   So, Your Honor, what we really have left is a couple of

4   issues, which are still significant. I would like to address

5   those.

6   The first remaining category of discovery that is still

7   outstanding is information regarding the extent of the

8   distribution of child pornography while the FBI was operating

9   the website. I do think it is an important distinction here.

10 I notice in the government's responsive reply at page 12, that

11 they characterize the situation as one where the government

12 allows the website to continue operating for what they

13 characterize as a brief 14-day period. I am not sure 14 days

14 is all that brief. But really my main concern is we are not

15 dealing with a situation where -- for example, the website was

16 under surveillance, and the FBI was developing probable cause

17 or inquiring into the investigation, watching the activities

18 of others. This was not a situation where they allowed the

19 website to continue; they actively operated and took control

20 of it. So there's a certain amount of ownership here that

21 that sort of passive plan does not capture, and I think it's

22 certainly important for understanding the thrust of our motion

23 to dismiss the indictment.

24   Once the FBI took control of the server on February 19th,

25 they owned it. They had the choice of shutting it down at

1 that point, investigating through whatever records were

2 already in the server. They also had the choice, for example,

3 to continue to operate it but blocking access to the actual

4 illicit content.

5   We have seen other cases where they have left certain

6 links or descriptions up, or suggestive material, but have

7 blocked user's ability to actually download or view the

8 illegal content. So this is really a bird of a different

9 feather, because during that entire 14-day period that this

10 was in fact an FBI website, there was continuous posting and

11 distribution and redistribution of child pornography. And I

12 do believe that's unprecedented, at least in my experience.

13   And I would note, Your Honor, that in terms of the

14 legality of this whole thing, and not to start arguing the

15 motion to dismiss, but really just in terms of why we are

16 seeking information about the extent of this distribution is

17 because there are a number of legal permissions which preclude

18 the government from doing this.

19   In fact, one of them was cited, and I overlooked it

20 previously in the government's briefing, at page 4, note 2,

21 under 18 U.S.C. 3509(m), the government is supposed to retain

22 custody and control of any child pornography that is seized

23 during an investigation. And of course that's not at all what

24 happened here.

25   So Your Honor, I really defer to the Court on this,

1   because ultimately what we are driving at is we want a factual

2   basis to support our motion. And really the question is, how

3   much does the Court need?

4   The undisputed facts I think at this point are that there

5   were over 200,000 members on this site; that tens of

6   thousands -- I estimated approximately 80,000 visits were paid

7   to the site during the period that it was under FBI control.

8   And we have used various adjectives or numbers to describe the

9   quantity of child pornography that was available in various

10 subdirectories, subforms on the site as being thousands of

11 images, a massive quantity of images, massive quantity of

12 videos.

13   I think in terms of the extent of distribution, the Court

14 could safely assume from all that that it was indeed a massive

15 quantity of illicit content. But our main thrust in terms of

16 getting more exact figures, if the Court is going to make

17 findings about how extensive this operation was and the

18 degree, we submit, to which the government was violating the

19 law in various respects, it may be important to have a more

20 specific count, and that information in terms of how many

21 people actually visit the site. And we know that many people

22 probably visit that site but did not necessarily look at

23 content, illicit content.

24   And it is really up to the government at this point I

25 think to choose their poison. If they want to disclose the

1 numbers of people who actually went into the various

2 subdirectories to look at content, and how many visitors were

3 doing that, I think that may be helpful. Otherwise I am more

4 than happy to stand on the assumption that there was a massive

5 amount of material distributed.

6   What I do not want to happen, though, and what I'd ask the

7 Court to one way or another foreclose, is to get to the

8 suppression hearing and potentially having witnesses for the

9 government trying to minimize how much content was

10 circulating, because I don't think from what we've just seen,

11 in terms of the characterizations in the government's own

12 pleadings, that it was a minimal amount of illicit content.

13   If the government does not want to essentially concede or

14 stipulate that there were tens of thousands of visitors, and

15 that there was a massive quantity of child pornography in

16 circulation, I do think we need more specific information.

17   Now, Your Honor, again, going on to the remaining issues,

18 the government's memoranda and sort of internal assessment --

19 assessment of both the legality of running an undercover

20 online operation like this, and also the Rule 41 issues,

21 whether the NIT warrant in particular was legal, it is again

22 in some sense the government's choice here. And we seem to be

23 viewing the same facts in a slightly different perspective.

24   I believe -- and I don't want to speak for the government,

25 but what I believe from their pleadings is that they are

1 taking the position that the fact that there was internal

2 Department of Justice or FBI counsel review of the NIT warrant

3 is relevant to the good faith analysis in terms of the

4 exception to the suppression rule. And as a legal principle,

5 that is correct, it would normally be the case.

6   But we are in a slightly different situation here because

7 one of our primary suppression arguments is specific to Rule

8 41 issues, and that is whether there was a deliberate

9 disregard of the law or Rule 41, specifically. And that has

10 nothing to do with the good faith exception. It is just

11 whether or not the government knowingly proceeded to submit a

12 warrant application that it was aware was inconsistent with

13 the law.

14   Now, I believe again from the submissions that we've made

15 to the Court, and what is publicly available in terms of DOJ's

16 own analysis of the scope of Rule 41 and the sensitivity of

17 online undercover operations, that we have enough in the

18 record to say that there's no way that this was some sort of

19 rogue operation, or DOJ did not make a conscious choice to

20 pursue the NIT warrants despite the fact that at best the Rule

21 41 arguments that have been offered in justification of that

22 warrant are questionable.

23   Now, then the question is again, what are we going to see

24 at the suppression hearing? It is simply a matter that the

25 NIT warrant in particular, and the whole website operation,

1 continued operation by the FBI, were the various points

2 reviewed and approved internally? We can take that as a

3 given. Frankly, I believe that helps our argument. That

4 establishes the deliberate nature of the actions. And then it

5 is up to the Court to determine whether they were legal or

6 not.

7 What I don't want to happen is for the government then to

8 put up witnesses to start talking about that internal process,

9 as they characterize them, consultations, in an effort to

10 persuade the Court, well, a certain number of DOJ attorneys

11 signed off on this, Your Honor, and therefore it must be

12 legal.

13 And if we are going to start drifting in that direction,

14 then I would be very much surprised, given what we know about

15 DOJ's own analysis of Rule 41, that there wasn't some dissent

16 or discord or other things going on in that consultation

17 process that we should be allowed to explore.

18 If that is where the government is heading for purposes of

19 the suppression hearing, then as we submitted in our reply

20 briefing, that seems to me to be a waiver of any privileges

21 that they are claiming.

22 So Your Honor, I really think at this point, having

23 resolved the programming code issue, our request is to put it

24 to the government, a choice on these two issues.

25 One, if there isn't going to be any disagreement that

1 there were tens of thousands of users accessing child

2 pornography through the various subdirectories, and that a

3 very large -- a massive amount of illicit content was

4 distributed, and the Court deems that sufficient to make

5 findings, then we can probably leave it at that.

6   If there's going to be any issue about the scope of it, or

7 if the Court believes more specific numbers are needed, then

8 we'd ask the Court to grant our motion.

9   I would just note, I think we addressed this briefly, we

10 cannot get that information, at least as far as -- from the

11 virtual website, at least as far as I was able to explore what

12 was on there and what was told to me by the FBI agent and the

13 AUSA, who were in the room with us, which is basically what

14 you see is what is available through this virtual website.

15 Most or all the information we are seeking is on the

16 government's server behind the website. We do not have access

17 to that.

18   And then the same choice that I indicated comes to this

19 issue of the internal consultations. There was simply an

20 approval process for this entire operation and the NIT

21 warrant. I do not think we will next -- we will need more

22 discovery on that if there's going to be any attempt by the

23 government, either in its responsive briefing or at the

24 hearing, to suggest -- to go into the details of the

25 consultations to suggest that that is somewhere out under --

1 reenforces or underscores the legality of what we are

2 challenging, then we feel we are entitled to full disclosure

3 of all those internal consultations.

4   Thank you, Judge.

5   THE COURT: Thank you, counsel.

6   Mr. Becker.

7   MR. BECKER: Thank you, Your Honor.

8   May it please the Court, I think a bit lost here in the

9 argument to this point is the legal background pertaining to

10 Rule 16 and criminal discovery, and then the good faith

11 exception, which is really the premise on which the defense

12 makes its other request.

13   The defendant's motion here really seeks to turn the

14 criminal discovery process on its head. By requesting

15 information that is not material to his defense of the actual

16 charges in this case, information that is specifically

17 exempted from production by Rule 16 itself, and on a theory

18 that has been -- a theory of discovery that has been

19 specifically rejected by the Supreme Court.

20   So let me go through with that first. As the Court is

21 well aware, discovery pursuant to Rule 16 must be material to

22 a defendant's defense. It is the defendant's obligation to

23 set forth specific facts to show that materiality. Rule

24 16(a)(2) specifically excludes the discovery or inspection of

25 reports, memoranda, or other internal government documents

1 made by an attorney for the government or other government

2 agent in connection with investigating or prosecuting the

3 case. That rule is amplified by the Supreme Court's decision

4 in *United States v. Armstrong*, which we cited in our

5 responsive briefing.

6   In that case the Supreme Court interpreted Rule 16 in a

7 way that forecloses the sort of requests for internal

8 government memoranda and deliberations that are being made

9 here. The Supreme Court interpreted defense, under Rule 16,

10 to be limited to claims that refute the government's arguments

11 that the defendant committed the crimes charged. Defense

12 means defense on the merits, a defense to the evidence that is

13 going to be presented by the government at trial pertaining to

14 him.

15   In *Armstrong*, the defendant raised a selective prosecution

16 claim similar to the sort of motion to dismiss based on this

17 allegation about outrageous government conduct, as made here,

18 and requested discovery about the government's prosecutor's

19 strategy.

20   THE COURT: You don't think that the question of

21 outrageous government conduct, if not granted on a motion,

22 would not be presented to a jury at trial?

23   MR. BECKER: I don't believe that it could be, Your

24 Honor. It is not a merits defense. And I don't believe it is

25 the sort of defense that could be submitted to a jury at

1 trial, nor has the defendant suggested that or submitted any

2 sort of briefing making that argument that I know of.

3   Now, of course, we haven't yet had our opportunity to

4 respond to the defendant's motion to dismiss. That response

5 is due on the 21st. We will respond on the merits of that

6 claim.

7   THE COURT: I am thinking ahead to the trial, and if

8 that is not a legal defense to be presented to a jury, it

9 might, in the hands of a good lawyer, lead to a jury

10 nullification, if not an argument to -- you know, the jury

11 could decide this is just unfair and determine not to convict.

12   MR. BECKER: Those seem like good reasons for the

13 Court to properly instruct the jury not to consider those

14 sorts of arguments or those sorts of considerations, Your

15 Honor, which are not merit defenses here.

16   The defendant is charged with receiving and possessing

17 child pornography. And ultimately the fact that the website

18 that he accessed was under government control, at "a" time

19 when he accessed it, and of course the defendant accessed that

20 website and registered on it long before the government seized

21 it. But the mere fact that the defendant also accessed the

22 website while it was under government control, it has no

23 bearing whatsoever on the merits of receipt and possession

24 charges based upon information found on his computer pursuant

25 to a search.

1   The motion to dismiss the indictment here, we would argue,

2   is so totally separate and apart from any sort of merits

3   defense. But even in that event, Your Honor, I want to bring

4   us back to the legal framework, because I really do believe

5   that *Armstrong* forecloses these sorts of requests. But even

6   if we look at the request -- I can quote particular language

7   from *Armstrong* if the Court thinks it is helpful. It is 517

8   United States 456, pages 462 and 463. In rejecting the

9   defense argument in that case, the Supreme Court stated

10 "because we conclude that in the context of Rule 16 the

11 'defendant's defense' means the defendant's response to the

12 government's case-in-chief. While it might be argued that as

13 a general matter, the concept of a 'defense' includes any

14 claim that is a 'sword' challenging the prosecution's conduct

15 of the case, the term may encompass only the narrower class of

16 'shield' claims, which refute the government's arguments that

17 the defendant committed the crime charged."

18   So I won't belabor that point any further, Your Honor, but

19 that's the Supreme Court very directly saying defense means

20 what evidence is presented at trial and how are you defending

21 against it, not an attack on the conduct of a government

22 investigation generally.

23   Now, in terms of the seizure of the website, first let's

24 get some facts correct. The FBI -- the government did not

25 create this particular website at issue. It operated for six

1 months before it was seized by law enforcement. It operated

2 for another two weeks under law enforcement control.

3   Now, I don't believe that a policy argument about whether

4 or not the government should interdict particular criminal

5 activity by particular criminals is relevant and that it in

6 fact brings to bear some potential serious separation of

7 powers issues in terms of the government's discretion to

8 investigate particular criminals using particular

9 court-authorized investigative techniques.

10   But that aside, this is not something the government

11 created. And if we are going to talk about the reasons why

12 this happened, is it possible that the government could have

13 shut that website down the day it was seized? Yes, of course

14 that's possible. But that ignores the rest of the context of

15 how this site operated.

16   This was a site that was created by its users. It is an

17 online bulletin board. It is helpful, I think, in

18 understanding that to think of an offline bulletin board, just

19 how does a regular bulletin board work? It is set up and

20 placed on a wall by some administrator. Then the users are

21 responsible for posting messages onto it and replying to those

22 messages. The users post messages and content within the

23 context of whatever categories are set up by the person who

24 first sets up that bulletin board. User-provided content,

25 that is how this works.

1   So it was and is the users of this particular website, in

2 the online context, who populated its content with messages,

3 including messages that had images and videos of child

4 pornography in them, and also messages that provided links,

5 that is online links to other places on the Internet where its

6 users could go and download child pornography using passwords

7 provided by the users of the site. So the child pornography

8 that was trafficked on this site was user-created and

9 user-tracked.

10   I think the use of the term "distribution" is loose and

11 not specific enough to the context here of a website whose

12 content was user-populated.

13   So again, there's no dispute here that as of the time the

14 government seized the site, and for the next two weeks, it was

15 possible and users did, like ██████, access child

16 pornography through that website. That is not in dispute and

17 won't be in dispute at any hearing on the motion to dismiss.

18   The defense is well aware of this. They have filed their

19 motion to dismiss largely based upon that premise. And we

20 don't believe that further discovery of the users, of other

21 users than the defendant, is necessary in order to make that

22 sort of argument, to the extent that information about other

23 users and whether they downloaded images or not is even

24 attainable. Of course, again, if we don't define our terms we

25 end up in a difficult situation. Users might save child

1 pornography that they accessed on their screen. They might go

2 to another website and download it or not.

3   We are not disputing -- the government is not disputing

4 that child pornography was accessible during the period that

5 the site was operated. We don't think, and absent a finding

6 by Your Honor, that further information is necessary.

7   THE COURT: Do you have -- what they asked for here

8 was, as I understand it, the total number of pictures and

9 videos that were downloaded and distributed, and the number of

10 visitors to the site during the subject time. Is that

11 information you have?

12   MR. BECKER: The number of visitors to the site

13 during that time period is information that we would have.

14   THE COURT: Why don't you give it to them; what's the

15 difference?

16   MR. BECKER: The difference, we don't believe that it

17 is relevant and material in the case, Your Honor. That's our

18 position. That information is available.

19   THE COURT: I am always suspect of a government

20 lawyer that says something is not material or relevant to the

21 defense. You are not in a very good position to determine

22 that question. You have to put yourself in their mind. You

23 have to come to that question with the mind and background of

24 a seasoned criminal defense lawyer to make that determination.

25   MR. BECKER: Well, here, Your Honor, the

1 determination is in the context of a specific motion that has

2 already been filed for specific reasons.

3   I certainly understand the difficulty in a prosecutor

4 taking the mind-set of a defense counsel. But we are not

5 exactly in that context here. The defense says this is

6 relevant to the motion they have already filed, which already

7 alleges outrageous government conduct based on information and

8 actions they know occurred, which is that the government

9 seized and continued to operate the website for two weeks, and

10 that child pornography continued to be available.

11   So I absolutely understand Your Honor's admonition on that

12 point, but I do think the context of this request makes it a

13 bit different.

14   That said, if the Court finds that we should provide the

15 number of visitors to the site, we can provide that

16 information. We will comply with the Court's order.

17   THE COURT: Do you have also the total number of

18 pictures and videos that were downloaded or distributed from

19 that website?

20   MR. BECKER: That information is not available for a

21 variety of reasons, Your Honor, that have to do with how the

22 site operates and how individual users could have and would

23 have used it.

24   So when I access a web page, there are innumerable ways in

25 which I might save that material to my computer. I might

1 right click a picture and click "save." I might take a screen

2 shot of a particular image and save it that way, similar to

3 taking a picture of your computer screen.

4   There's just not a way for the government to give an

5 accurate count of exactly how each user interacted with the

6 site and to what extent the user saved images that were

7 available.

8   Further, because of the way the administrator set this

9 site up, there were links available to external websites that

10 contained child pornography, which the users could then go to

11 and download from. Those external websites were not within

12 government control, and so we are not able to provide

13 information as to what an individual user might have done with

14 those sorts of images or videos.

15   THE COURT: You know, Mr. Becker, I might say if this

16 was only this defendant and the argument was outrageous

17 government conduct, it would be a much different argument than

18 if this was 10,000 people, in terms of whether it was

19 outrageous or not.

20   I mean, it's one thing to go after one person that you

21 think is committing a crime, and something different to go

22 after everybody under the sun under the same premise.

23   MR. BECKER: Your Honor, respectfully, I am not sure

24 that I follow that rationale, because if there's one person

25 committing a crime, or 10,000 people committing crimes, we, as

1 the government, have an obligation to investigate all 10,000,

2 not just one.

3   So I think it is a logical fallacy to say here that

4 somehow it is the government's fault that thousands of

5 criminals gathered at this website to exploit children via the

6 trafficking of child pornography. The government did not

7 create that. The government responded to this massive website

8 trafficking in criminal activity in order to try to actually

9 find, identify, and bring to justice the people who were using

10 it criminally. And so --

11   THE COURT: How many people have you charged in this,

12 off of this website?

13   MR. BECKER: I can provide that information, Your

14 Honor. I am leery of providing that information in a public

15 forum given the ongoing nature of the investigation, but I do

16 have numbers that I can provide to the Court.

17   But again, my point is, Judge, this was a massive scope of

18 criminal activity which required the government's response

19 here. It is hard, I think, to say to prosecutors and agents

20 who see users gathering in such a massive scale in a way that

21 makes -- and for the record, we are talking about the

22 anonymous Tor network here. They are gathering in a means and

23 a way that makes their identification extremely difficult.

24   So could the government have just shut that website down

25 as soon as it was seized? That is possible. That is one

1 thing the government can do. And what happens next? All of

2 those criminal users, who are using this website in order to

3 traffic in child pornography amongst themselves, simply go and

4 set up another website and continue to engage in the exact

5 same behavior that continues to exploit children in the same

6 way.

7   The only way for the government to actually stop this sort

8 of conduct is to take action, to identify and apprehend the

9 perpetrators. That is what the government did in this case.

10 The government explained that to the judges who authorized the

11 techniques, both in the network investigative technique

12 affidavit and in the wiretap affidavit pertinent to the

13 investigation.

14   It is unfortunate that there are so many thousands of

15 criminals who act similarly, but that is not attributable to

16 the government. That is attributable to the criminals who

17 engage in that behavior.

18   I apologize, Your Honor, if my tone is too forceful. I

19 have only appeared in your courtroom twice, Your Honor. This

20 is what I do. It is obviously something that I am

21 particularly passioned about as a prosecutor. I mean no

22 disrespect whatsoever to the Court.

23   THE COURT: I understand, Mr. Becker. The other side

24 of that coin obviously is that investigations have to be

25 within the limits of the Constitution, no matter how bad the

1 crime is.

2   MR. BECKER: Absolutely, Judge. Absolutely. And

3 here the NIT was authorized by a magistrate; the wiretap was

4 authorized by a United States District Court judge with full

5 knowledge and understanding of the overall investigative

6 strategy.

7   THE COURT: Okay, go ahead.

8   MR. BECKER: So I will move, Judge, to the good faith

9 side and the internal government deliberative documents

10 pertaining to that.

11   So the good faith argument here is premised on law

12 enforcement's objectively reasonable reliance upon the

13 authorization of a magistrate. And the government has asked,

14 and will ask, the Court to find that the good faith exception,

15 the *Leon* exception applies.

16   The good faith exception is not based upon review of

17 internal government deliberative memos. It is based upon a

18 magistrate authorizing the NIT warrant in this case, as did

19 occur. We don't believe that in any way brings to bear

20 internal government deliberative documents.

21   We certainly do expect there would be testimony or

22 evidence that the affiant in this case consulted with an

23 Assistant United States Attorney before presenting the warrant

24 to the magistrate, as is the required procedure in every

25 single United States Attorney's office that I am aware of.

1 And I have been in about 25 different districts around the

2 country.

3   That is obviously a very different premise than anything

4 that brings to bear internal government deliberative memos.

5 So it seemed to me that what I heard today from the defense is

6 that we don't have an issue here that requires compulsion of

7 any of those memos, unless and until there was some argument

8 other than that. And I don't believe we'll be in that

9 position, or are in that position, Your Honor.

10   So I do expect evidence that the NIT warrant was submitted

11 to, approved by an Assistant U.S. Attorney. I don't expect

12 there to be any presentation that somehow there was also other

13 deliberations by the Department of Justice that bear on that

14 good faith inquiry.

15   So I am a little bit at a loss, I guess, to speak any more

16 than that, to the sort of speculative concern that that might

17 happen.

18   THE COURT: Let me ask you something here: In light

19 of the statutes that makes some things undiscoverable, if you

20 present evidence at a suppression hearing, for example, that

21 the warrant was approved by a United States Attorney, aren't

22 you opening up that whole thing, the whole thing they are

23 looking for? Or don't you have to -- if you want to protect

24 that particular statutory or rule privilege, don't you have to

25 just say here's the document, and does it pass constitutional

1 muster without a bunch of evidence about the process that it

2 went through?

3   MR. BECKER: I don't believe that is correct, Your

4 Honor. It is a well-established principle in the Ninth

5 Circuit, as elsewhere, that one of the factors in the good

6 faith analysis is whether or not a law enforcement agent

7 consulted with a prosecutor before seeking the warrant. I

8 don't believe that the mere fact that that occurred brings to

9 bear internal deliberations of government attorneys.

10   I think the only means in which, or way in which I think

11 that might bring to bear internal deliberations would be if

12 there were a *Brady* request, for example. So if the defense

13 were to request *Brady* material about whether any government

14 lawyer told the affiant that the warrant was not legal, and if

15 there were materials responsive to that request. In that

16 event we might need to disclose them.

17   But outside that context -- that sort of context, Your

18 Honor, no, just the mere factor of having checked with a

19 prosecutor doesn't then bring to bear other internal

20 deliberative memos. We just don't think that follows at all.

21   THE COURT: Why is that even relevant if there's an

22 attack on the affidavit supporting the search warrant?

23   MR. BECKER: Well, again, the Ninth Circuit has

24 identified that as one factor in the analysis. So the Court

25 will evaluate: did the law enforcement agent act in

1 objectively reasonable reliance on the authorization of the

2 magistrate?   So in determining whether the law enforcement

3 agent's reliance was objectively reasonable, having run it by

4 a prosecutor, consulted with an attorney, is one factor the

5 Ninth Circuit says the Court should consider, and an important

6 factor the Ninth Circuit says this Court should consider.

7   THE COURT: That's on the other end of the analysis,

8 it sounds like. You don't get into the good faith exception

9 unless the underlying warrant was not a good warrant.

10   MR. BECKER: That's correct, Your Honor.

11   THE COURT: You are not submitting that here, are

12 you?

13   MR. BECKER: No, absolutely not, Your Honor. And

14 again, good faith only comes into play if the Court determines

15 that the warrant did fail legally.

16   We are not conceding that. This is just -- this is what

17 the defense says this particular set of information is

18 relevant to, and that's why we are arguing it in that context.

19   So Your Honor, if the Court has no further questions for

20 me, I will rest for now.

21   THE COURT: I don't.

22   MR. FIEMAN: Just briefly, Your Honor. I would like

23 to start with the last point first, in terms of how the good

24 faith argument and the deliberate violation of Rule 41 that we

25 are alleging are just going to play out at the hearing.

1   I just want to be clear on the record, because I don't

2 want to get to the hearing and have this part of our

3 presentation or our strategy come as a surprise to the

4 government, because I don't think any of us is going to be

5 well served by that.

6   In my view, if the government is electing not to turn over

7 any of the consultation materials, and they want to stand on

8 the fact that the NIT warrant was reviewed and approved at

9 some point by an Assistant United States Attorney, we'll take

10 that. Because in my firm view, they are just backing

11 themselves into a corner.

12   What we did not want was the government to come in here

13 and say, well, this was prepared by an FBI agent, and although

14 their subjective knowledge isn't really relevant and good

15 faith is based on what a reasonable author should know about

16 the law, well, Your Honor, it was reviewed by an Assistant

17 United States Attorney and therefore good faith should apply.

18   Our whole point is that DOJ has, from start to finish,

19 engaged in deliberate violations of Rule 41 and deliberate

20 violations of the law when it comes to trafficking and child

21 pornography. As long as they are going to say, yes, this is

22 the path we elected to follow, and then it is up to the Court

23 to determine whether it was legal, that's fine. But they seem

24 to be staking out a position that somehow these consultations

25 are going to help them on the good faith prong here.

1   The ultimate answer is already in our briefing. The good

2 faith exception is essentially foreclosed when it comes to

3 reliance on a warrant when the government itself is

4 responsible for the defects in the warrant. We are not

5 talking about some kind of close probable cause determination

6 where reasonable minds might differ about the facts and there

7 was an honest representation of information in the warrant

8 that the judge just happened to decide differently from a

9 reviewing judge. Our premise here is that this entire

10 operation is ripe with misleading and false statements and was

11 done in deliberate violation of the policies that DOJ has

12 about the parameters of Rule 41, and ultimately lead to what

13 appears to be an unprecedented engagement in illegal activity

14 in terms of distribution from the website.

15   That is a very unusual set of facts. And I think it is

16 very important, before we start squabbling at the suppression

17 hearing about where certain issues are going, that I at least

18 make that statement to the Court and the government about what

19 our intentions are.

20   If the government at this point wants to assert that we're

21 applying privilege and their condition is we are simply going

22 to stipulate or state that this NIT warrant was approved by a

23 DOJ attorney at some point and we leave it at that, we'll take

24 that. We'll take that, Your Honor.

25   Now, Your Honor, in terms of just -- the other points in

1 terms of the remaining disclosure about activity on the site,

2 one premise here I think we need to just put aside completely

3 is that the government keeps presenting to the Court the

4 notion that the alternative was to either shut down the

5 website or do an investigation that involved distribution of

6 child pornography. And that is simply not the case.

7   There are a lot of unanswered questions here. Why, if a

8 NIT could be deployed at any time somebody clicked on any

9 aspect of the website, including their home page, did they

10 choose to make it -- excuse me, choose to continue to

11 distribute child pornography? I mean, their whole premise is

12 there was probable cause from the time he signed on to this

13 website.

14   And one of the things we intend to explore, in terms of

15 the outrageousness of the government conduct, is that even

16 though by their own statements this investigation could take

17 place just by clicking on the various aspects of the site,

18 there's no necessity to download or distribute this content,

19 as far as I can tell from their own analysis of how probable

20 cause was supposed to operate in this case.

21   Now, of course we are challenging the very notion that you

22 have probable cause at the time of signing in, because this

23 does appear to be a child pornography website, to an

24 uninformed viewer. But certainly we've also said there are

25 other aspects which clearly did have content. And this could

1 have been refined in such a way that they had their probable

2 cause and had deployed their NIT all properly and in a

3 suitably refined and focused manner without requiring the

4 distribution of child pornography. And that is where the

5 outrageousness truly comes in, because while I appreciate

6 Mr. Becker's passion about the importance of this

7 investigation, and I understand that, it is not as if the

8 government didn't have myriad ways to focus and narrow this,

9 as they have done in other cases.

10   That is also partly what makes this unprecedented, is that

11 they chose to do this in an extraordinarily expansive way in

12 terms of the number of targets, or potential targets, and in

13 terms of not trying to restrain what was ultimately ending out

14 on the Internet.

15   And the Court has already seen there are other

16 pronouncements about how even viewing one of these images is

17 supposed to be so damaging to the victims in these cases and

18 there truly are victims. But the question is, how do you

19 handle your resources in the course of an investigation?

20   I have never seen anything like this, and that is all

21 there is to it. I have never seen where the government has

22 just sprayed the Internet or a neighborhood or in a gun

23 investigation, a drug investigation, this kind of uncontrolled

24 dissemination of contraband. And that is really what we are

25 trying to drive at, what really is the extent of this.

1   Now, Your Honor, turning to my Exhibit 2, very briefly,

2 the October 22nd letter, I would just like to run very quickly

3 down what's outstanding at this point.

4   We asked for the number of child pornography pictures that

5 were posted on the site during the operation. That, I do not

6 believe the government can claim with a straight face they do

7 not have that information. That will be in their server.

8   That also goes to the second item, the number of videos

9 that were posted, also the number of links. I have had

10 clients who have been charged with possession of child

11 pornography for posting a link to a video, not necessarily

12 uploading the content. The government takes the view that

13 links constitute distribution. If there are links, as

14 Mr. Becker has said, those should be included in the count.

15 That information is in the government server.

16   They would also be able to tell user by user, as they did

17 with ████████ , what videos or links were viewed.

18   I understand Mr. Becker's argument about the downloading;

19 it is true, there are various ways to preserve. You can

20 screen shot. You can download. You may just view it, as the

21 Court has seen many of times, and the government will take the

22 position that viewing it is possession, because it ends up in

23 a temporary cache once it appears on the screen.

24   If they can't give us an exact number, I am sure they can

25 ballpark that. That is also going to be available in the

1 server, as I know from prior cases.

2   The number of visitors, I think the government is going to

3 give us. But I would ask for a breakdown on that, as we very

4 much clearly indicated to the Court at this point, not

5 everybody who went to that site, particularly given its home

6 page as it actually appeared at the time the FBI was operating

7 it -- I don't believe everybody was necessarily looking for

8 child pornography. They have identified various

9 subdirectories that were clearly dedicated to child

10 pornography. If they want to refine the count in that regard,

11 that's fine; that should still be extremely helpful.

12   And Your Honor, turning to page 2, we asked for a summary

13 of any measures that the FBI took to limit access or to block

14 images. My understanding at this point is that there were no

15 such measures whatsoever taken.

16   THE COURT: You refer to page 2 of --

17   MR. FIEMAN: I'm sorry -- of our October 22nd

18 discovery request letter, which is Exhibit 2, Your Honor.

19   We do not need additional discovery if the government's

20 position is that whatever the FBI allowed or uploaded during

21 that time, all of it was accessible. That kind of answers our

22 question.

23   And you know, Your Honor, there is an issue about why the

24 site was kept up and running as long as it was. They keep

25 referring to the 14-day period that the FBI was operating the

1   site is brief, and of course the Court will characterize it as

2   it sees fit.

3   I can tell you I have had clients charged for much briefer

4   interactions with websites, often amounting sometimes to only

5   a few images. So I don't know whether there was a point to

6   where DOJ came to the realization that maybe this was going

7   too far, or they simply decided they had identified enough

8   targets, but I do believe that the reasons for the duration of

9   this distribution will be relevant to the hearing.

10   And the last item, I think I have addressed, in terms of

11 the documentation regarding their internal procedures on this.

12   Your Honor, when we're talking about the typical case and

13 the typical good faith argument in the context of a probable

14 cause determination, this just isn't the typical case. From

15 what we've made out so far, there is no legal exemption for

16 what the government did here. You know, there's -- Rule 41

17 doesn't allow for this. There's no statutory exception for

18 the government to distribute child pornography in the course

19 of trying to make a case.

20   The number of people, 200,000 users, targeted from a

21 single warrant, I think is unprecedented.

22   We are dealing with a number of very unusual factors in

23 this case, and I think it is important to bear in mind that

24 while the government keeps going back to *Armstrong* and talking

25 about discovery in terms of defense at trial, we've given you

1 the Ninth Circuit law, Your Honor, which says that all

2 information that relates to pretrial motions is relevant to

3 the defense.

4 More importantly, we are not required to project our

5 strategy at trial. There are a host of issues percolating in

6 here that we intend to put before a jury. We will not --

7 obviously because we are not allowed to -- be asking for a

8 nullification instruction. But there are, if nothing else, a

9 host of issues about *res gestae* and the context of how

10 ███████ was even targeted, that are inevitably going to

11 come up in this trial, unless the government is going to

12 streamline its case to the point where they won't be able to

13 lay the foundation for a lot of their materials. This is all

14 directed onto ████████'s overall defense but the inevitable

15 issues that are going to be coming up at trial.

16 Finally, Your Honor, as indicated in our briefing,

17 materiality is a very low threshold. We just need to show

18 that this is relevant to either a pending motion or defense at

19 trial. And I think the Court has grasped kind of where we are

20 heading, that I don't need to belabor that.

21 Unless you have any questions, Your Honor, we would ask

22 for the specific relief that we requested in our motion.

23 THE COURT: Well, let me address the limitation,

24 first. Rule 16, the Federal Rules of Criminal Procedure -- it

25 is hard to cite these things because there are so many sub

1   parts. I guess it is (a)(2) of that rule provides that the

2   rule does not authorize the discovery or inspection of

3   reports, memoranda, or other internal government documents

4   made by an attorney for the government or other government

5   agent in connection with investigating or prosecuting the

6   case. It seems to me that that is a rule that binds the

7   Court.

8   And the government in responding to the order that I am

9   going to make, I think can recognize that exception and

10 obviously in good faith withhold things that come within that

11 definition. The problem with that, that I see, is that in a

12 suppression hearing, if the government withholds those

13 documents, that an agent, for example, might be able to

14 testify that he conferred with counsel. You start talking

15 about what the lawyer said, all of a sudden that's all open.

16 It is a fine line to walk. Once an agent says, well, the

17 government lawyer told me this is all good, well all of a

18 sudden that is open, it seems to me. But as I indicated, I

19 think you can withhold that information that comes within that

20 category.

21   Other than that, I think that the items requested should

22 be provided. And if they can't be specifically -- I am

23 referring to the October 22, 2015, letter to Ms. Vaughn from

24 Mr. Fieman, and I think those things should be produced by the

25 government. I think they are reasonably relative to defense

1   theory in the case and material to that theory, giving the

2   benefit of the doubt to the defendant on that question.

3   I understand that some of the specific things requested

4   may not be readily available, but as requested in that letter,

5   if the exact figures or totals are not readily available, a

6   good faith estimate of the numbers would be sufficient.

7   If specifics are not available, I think also the number of

8   charges arising from this investigation should be -- the

9   numbers, only numbers, I am saying -- should be provided to

10   the defense.

11   Is that clear enough? The motion should be granted to

12   that extent, and denied to the extent that the production

13   would run afoul of Rule 16(2).

14   MR. FIEMAN: Two quick clarifications.

15   One is, if we could get an estimate -- I understand that

16   the government may need some time to figure out how to capture

17   this, but if we could have an estimate of how much time they

18   need to keep things moving forward because we do have a

19   hearing scheduled.

20   MR. BECKER: Is the Court going to issue a written

21   order specifying what we are to provide?

22   THE COURT: Do you need one?

23   MR. BECKER: I think that would be our preference,

24   Your Honor, just so we are clear, because I think --

25   particularly with respect to the site statistics. I think I

1 understand what the Court is ordering. That last request on

2 that letter that pertained to steps taken by the government to

3 limit dissemination, we would like to be clear on what it is

4 we are to produce and by when.

5   THE COURT: Well, I will issue an order later today.

6   MR. FIEMAN: Your Honor, I'd understood that

7 basically the Court was granting everything -- that everything

8 in our October 22nd letter should be produced, with the

9 exception of the consultations and memoranda records that were

10 separately issued on one subheading, and that was with the

11 proviso that the government may actually open the door to that

12 or should avoid opening the door to that discovery at the

13 hearing.

14   THE COURT: Well, I don't need to go that far. It is

15 a matter for the trial judge, who probably will be me, but at

16 my age, who knows.

17   MR. FIEMAN: Well, Your Honor, in that case, maybe we

18 should move up the hearing; we have got a lot before the

19 Court.

20   THE COURT: Okay.

21   MR. BECKER: Judge, I guess -- I think our next

22 motion hearing is scheduled for, I believe, the 22nd of

23 January.

24   THE COURT: I think so.

25   MR. BECKER: I guess I would request the first week

1 of January in terms of providing a response. And if we can

2 provide it sooner, we'll do so. Obviously we have some

3 holidays coming up, and I do need a chance to confer with

4 supervision as to some of the aspects of the Court's order.

5   MR. FIEMAN: That will be fine, Your Honor, thank

6 you.

7   THE COURT: All right. Okay. So that would end the

8 hearing, and I will issue an order this afternoon or maybe

9 later this morning.

10   MR. FIEMAN: Thank you, Judge.

11   (Proceedings concluded.)

12

13

14   *   *   *   *   *

15   C E R T I F I C A T E

16

17   I certify that the foregoing is a correct transcript from

18 the record of proceedings in the above-entitled matter.

19

20 /S/ Teri Hendrix_____   December 16, 2015

21 Teri Hendrix, Court Reporter   Date

22

23

24

25