

JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF WASHINGTON  
AT TACOMA

UNITED STATES OF AMERICA,	)	No. CR15-5351RJB
	)	
Plaintiff,	)	
	)	DEFENDANT’S REPLY TO
v.	)	GOVERNMENT’S RESPONSE TO
	)	THIRD MOTION TO COMPEL <sup>1</sup>
JAY MICHAUD,	)	
	)	
Defendant.	)	

**I. INTRODUCTION**

In its Response to Mr. Michaud’s discovery motion for the NIT code, the Government raises the specter of the defense “rummag[ing] through the government’s files[.]” Govt. Response (Dkt. 134) at 11; *see also id.* at 12, 19. The defense does not seek to rummage. To the contrary, the defense seeks three specific items, namely key components of the NIT code that the Government used to seize and store evidence from Mr. Michaud’s computer. Detailed descriptions of the missing data and their relevance to the defense were set forth in Mr. Michaud’s initial motion (Dkt. 115) and the accompanying declaration of expert Vlad Tsyркlevitch (Dkt. 115-1). The Government does not dispute the facts in the declaration or Mr. Tsyркlevitch’s qualifications.

<sup>1</sup> Mr. Michaud has filed two prior motions seeking discovery from the Government. *See* Govt. Response to Defendant’s Motion to Compel (Dkt. 134) at 1, n.1; *see also* Defendant’s First Motion to Compel (Dkt. 54) and Response to Motion to Seal and Motion to Compel Discovery (Dkt. 113) at 4. The Court has not yet ruled on the latter motion.

1 As a threshold matter, the Court should that the Government has already used its  
2 nondisclosure of the code data as both a sword and a shield, and the defense is  
3 concerned that the Government will do so again at trial if it does not make full  
4 discovery. Specifically, prior to the January 22 hearing, the Government assured  
5 defense counsel and the Court that it had provided “sufficient” code data for the  
6 pending suppression motions. *See* Govt. Response to Request for Expedited Hearing  
7 (Dkt. 123). Yet, during the suppression hearing itself, Government counsel objected  
8 several times to the testimony of Dr. Christopher Soghoian about how NITs work, on  
9 the ground that his opinion “isn’t based on any analysis of a network investigative  
10 technique in this case.” January 22, 2016 Hearing Transcript at 102; *see also id.* at 105.

11 The Court should not allow the Government to have it both ways, on one hand  
12 withholding relevant evidence, and on the other hand trying to prevent the defense from  
13 challenging the Government’s case because it does not have access to that evidence.  
14 This problem, which was previewed at the suppression hearing, will become only more  
15 acute at trial.

16 Further, as discussed briefly below, the Government’s understanding of the law  
17 pertaining to Fed. R. Cr. P 16 is deeply flawed and it would erect insurmountable  
18 barriers to discovery, where the defense would have to prove in advance exactly what  
19 the requested items do, simply in order to review them.

20 The Government also does not dispute that the defense has agreed to adopt  
21 rigorous security measures to preserve confidentiality, nor does it suggest that those  
22 measures are now inadequate. At the Government’s request, the defense has agreed to  
23 have just one defense expert review the code at a Government facility, subject to the  
24 special protection order that the Government itself submitted to the Court to ensure  
25 nondisclosure to outside parties or the public. *See* Dkt. 115 at 3, n. 1; Dkt. 96 (code  
26 data protective order). The Government has raised no objections to the qualifications or

discretion of the defense’s expert, and in fact (as noted in the defense’s motion to compel) Mr. Tsyrklevich has previously worked for law enforcement and national security agencies and maintained high level security clearances.

Finally, the Government has made no showing that it needs an *ex parte* hearing, *i.e.* that it cannot demonstrate in pleadings shared with the defense why the law enforcement privilege should bar otherwise-appropriate discovery. Accordingly, the discovery motion should be granted and the Government’s request for an *ex parte* hearing should be denied.

## II. RESPONSE ARGUMENT

### A. The Code the Defense Seeks is Material.

#### 1. The Code and Its Relevance.

According to the Government, the NIT code at issue in this case “consisted of computer instructions, to which Michaud has access, that produced particular results that have also been provided.” Govt. Response at 10. But as detailed in Mr. Tsyrklevich’s declaration (and as the Government is fully aware), an “NIT” is in fact a set of computer instructions, or components, that operate together to alter or defeat the security features on a target computer; locate and seize data on the target computer; and then transmit the data to a law enforcement facility for storage. *See* Third Motion to Compel, exh. A (Dkt. 115-1).

In this regard, the Government does not dispute any of the facts alleged in the expert declaration or his qualifications. Nor does it dispute that it has provided just part of one of the four NIT components.<sup>2</sup>

---

<sup>2</sup> Specifically, missing **Component “A”** “is critical to understanding whether the unique identifier used to link a defendant to access of illegal content is actually unique.” Tsyrklevich Declaration at 3. Mr. Tsyrklevich also explained that errors in components of this type “are pervasive in modern software.” *Id.*

**Component “B”** is an “exploit” that is intended to execute on the computer that is being identified” (i.e. Mr. Michaud’s computer) to override security features and exploit flaws

1 As a general matter, “[a] defendant needn’t spell out his theory of the case in  
 2 order to obtain discovery. Nor is the government entitled to know in advance  
 3 specifically what the defense is going to be.” *United States v. Hernandez-Meza*, 720  
 4 F.3d 760, 768 (9th Cir. 2013). Nevertheless, Mr. Michaud will briefly outline part of  
 5 his anticipated defense at trial in order to provide the Court more guidance in ruling on  
 6 this motion.

7 First, as discussed in the initial Motion, Mr. Michaud expects to challenge the  
 8 Government’s chain of custody regarding the supposed linkage between his computer  
 9 and “Website A.” In this regard, the Government has alleged that a site member named  
 10 “Pewter” spent many hours on the site and downloaded specific pictures from it, which  
 11 the Government intends to offer as evidence at trial. The Government has further  
 12 alleged that “Pewter” and Mr. Michaud are the same, based on data that the NIT seized  
 13 from Mr. Michaud’s computer. To counter these allegations, the defense intends to  
 14 challenge the accuracy of the identifying data that the Government claims connects Mr.  
 15 Michaud to both “Pewter” and specific activity on the Website.

16 Second, and equally importantly, the defense will challenge the Government’s  
 17 case by arguing to the jury that child pornography found on the computer or other  
 18 devices seized from Mr. Michaud’s home came from somewhere or someone else, or at  
 19

20  
 21 in the Tor browser. *Id.* This component is essential to understanding whether there were other  
 22 components that the Government caused to run on Mr. Michaud’s computer, beyond the one  
 23 payload that the Government has provided.

24 And, as Mr. Tsyklevich explains regarding **Component “D,”** the Government’s use of  
 25 data storage and the programming practices to avoid data corruption and tampering make  
 26 analyzing this component of the NIT essential to verifying the digital ‘chain of custody’ of  
 information derived from the NIT.” *Id.* at 3-4.

Finally, as to the “payload” (**Component “C”**), this runs on the target computer to  
 extract information from it. Tsyklevich Declaration at 2. Here again the Government does not  
 dispute the materiality of this part of the NIT, but it will not confirm if it has in fact produced  
 all of the “payload” component.

1 least that the Government cannot prove beyond a reasonable doubt that Mr. Michaud  
2 intentionally downloaded illegal pictures.

3 In this regard, it is now undisputed that the Government inserted “malware” onto  
4 Mr. Michaud’s computer that compromised and overrode its security settings.  
5 Therefore, either pornography from “Website A” itself was mistakenly or recklessly  
6 sent to his computer, or else the pornography came from other sources (such as viruses  
7 or remote users that gained access to the computer) after the security settings on Mr.  
8 Michaud’s computer had been compromised by the Government’s NIT.<sup>3</sup>

9 The Government itself asserts that “[e]vidence is ‘material’ under Rule 16 only  
10 if it is helpful to the development of a possible defense.” Govt. Response at 5, citing  
11 *United States v. Olano*, 62 F.3d 1180, 1203 (9th Cir. 1995). In fact, the Ninth Circuit  
12 has held that materiality is much broader: “Information is material even if it simply  
13 causes a defendant to ‘completely abandon’ a planned defense and ‘take an entirely  
14 different path.’” *United States v. Hernandez-Meza*, 720 F.3d 760, 768 (9th Cir. 2013),  
15 quoting *United States v. Doe*, 705 F.3d 1134, 1151 (9th Cir. 2013). But even taking the  
16 Government’s crabbed definition of materiality at face value, the discovery that is  
17 sought in this case is plainly “helpful to the development of a possible defense.”

18 Further, although the Government is correct that a defendant must present facts  
19 showing materiality, it seriously overstates what is required for that showing and to call  
20 the present request a “fishing expedition” is misguided. Govt. Response at 5. Mr.  
21 Michaud seeks not some unknown items, possibly contained (or not) somewhere within  
22 the Government’s files. He seeks instead clearly identified and specific categories of  
23 information that are in the Government’s possession, and which the Government

---

24 <sup>3</sup> In this regard, the Government has disclosed that some images related to Count III of the  
25 superseding indictment may not have come from “Website A.” However, at the same time, the  
26 Government does not know where the images actually came from or when they were  
downloaded. Additional forensic analysis by the defense will be needed to try to determine the  
source of these alleged images, and that analysis will largely depend on access to the NIT code.

1 concedes were used to alter the security features of Mr. Michaud's computer and then  
2 extract, transmit and store evidence that will be used at trial. "A party seeking to  
3 impeach the reliability of computer evidence should have sufficient opportunity to  
4 ascertain by pretrial discovery whether both the machine and those who supply it with  
5 data input and information have performed their tasks accurately." *United States v.*  
6 *Budziak*, 697 F.3d 1105, 1112 (9th Cir. 2012) (finding abuse of discretion in trial  
7 court's denying discovery regarding computer program).

8 *Budziak* is instructive for several reasons. First, the Ninth Circuit clearly viewed  
9 the request as far different from a "fishing expedition" because, as here, the defendant  
10 "specifically requested disclosure of the [relevant] program[.]" *Id.*

11 Second, as here, the defendant "identified specific defenses to the . . . charge that  
12 discovery on the [relevant] program could potentially help him develop." *Id.* The court  
13 observed that "access to the . . . software was crucial to Budziak's ability to assess the  
14 program and the testimony of the FBI agents who used it to build the case against him."  
15 *Id.*

16 Finally, the court warned, "In cases where the defendant has demonstrated  
17 materiality, the district court should not merely defer to government assertions that  
18 discovery would be fruitless. While we have no reason to doubt the government's good  
19 faith in such matters, criminal defendants should not have to rely solely on the  
20 government's word that further discovery is unnecessary." *Id.* at 1112-13.

21 Here, far from relying on speculation to justify discovery, Mr. Michaud is  
22 relying on facts already in the discovery, the un rebutted declaration of Mr. Tsyklevich,  
23 and early disclosure of an anticipated defense at trial. As to this proffered defense, the  
24 Government may respond by inviting the Court to assess the likelihood of its success or  
25 contend that it is unpersuasive. Setting aside the fact that juries, not prosecutors, must  
26 determine reasonable doubt, the Ninth Circuit has clearly held that it is not for the trial

1 court (and certainly not for the Government) to judge the strength of a defense. *Cf.*  
2 *United States v. Johnson*, 459 F.3d 990, 993 (9th Cir. 2006) (in determining whether a  
3 defendant is entitled to a jury instruction on a particular theory of defense, “we have . . .  
4 repeatedly stated that the defendant is entitled to his proposed instruction even if his  
5 evidence is weak, insufficient, inconsistent, or of doubtful credibility”) (internal  
6 quotation marks omitted). Moreover, defense counsel has successfully challenged the  
7 reliability of the Government’s forensic evidence, and its claim that a defendant  
8 knowingly downloaded pornography, in other cases involving computers that had been  
9 compromised by malware and viruses. And regardless, as already noted, discovery is  
10 material even if it just leads a defendant, after full disclosure, to abandon a defense.  
11 *Hernandez-Meza*, 720 F.3d at 768.

12 In addition, the Government errs when it argues that the defense has not proven  
13 that, for example, “the NIT interfered with or somehow compromised any data or  
14 computer functioning.” Govt. Response at 8. To the contrary, both Dr. Soghoian’s  
15 un rebutted testimony at the January 22 hearing and Mr. Tsyklevich’s uncontradicted  
16 declaration establish that the NIT inevitably compromised the computer’s security  
17 features. The extent of this problem is still unclear only because a full assessment  
18 cannot be done without examining the NIT code. The Government nevertheless seeks  
19 to turn the requirement that a defendant make a preliminary *showing* of materiality into  
20 a standard that the defense could almost never meet of *proving* materiality, when the  
21 proof itself is what the defense is seeking to review.

22 Under the Government’s approach, the defense would not be entitled to  
23 documents, for example, pertaining to a drug-detection dog’s training and certification,  
24 without first proving that there were problems in that training. Yet the Ninth Circuit  
25 has ruled squarely to the contrary. *See United States v. Cedano-Arellano*, 332 F.3d 568  
26 (9th Cir. 2003). There is no indication in *Cedano-Arellano* that the defendant made any



1 showing about the need for the documents, other than that the dog's reliability would  
2 inevitably be an issue at trial. There is certainly no suggestion that, in asking the trial  
3 court for discovery, the defendant could initially point to any flaws in the dog's training  
4 or reliability. Yet that is just what the Government insists a defendant must do to make  
5 a "showing" of materiality.

6 As to the defense's right to computer code that is relevant to data chain of  
7 custody issues, the same problems appear. The Government complains that the defense  
8 "presents no facts whatsoever to suggest that there are or were any issues with the so  
9 called "digital 'chain of custody'" pertaining to the NIT-derived information." Govt.  
10 Response at 11. Yet, at the same time, it offers no declarations or other evidence to  
11 challenge the defense's submission from its expert that explained how data encryption,  
12 transmission and storage are rife with potential problems and must be verified.

13 Under the Government's theory, because the defense cannot currently point to  
14 specific flaws in the chain of custody, it is not entitled to documents that will help it  
15 determine whether the chain of custody was secure and accurate. But this puts the  
16 evidentiary cart ahead of the discovery horse. Simply suppose the issue were discovery  
17 of paper records pertaining to the chain of custody for DNA samples, rather than  
18 electronic data, and the Government contended that "the defense is merely speculating  
19 that there may be problems with the chain of custody." This Court would reject such a  
20 position out of hand. There can be no question that items relevant to a chain of custody  
21 are discoverable, without the defense first having to show defects in the chain. *See,*  
22 *e.g., United States v. Brewster*, 2009 WL 804709 (D. Idaho Mar. 27, 2009).

23 Finally, the Government argues that the District Court decision in *United States*  
24 *v. Rigmaiden*, 844 F. Supp. 2d 982 (D. Ariz. 2012) is "instructive" because it denied  
25 discovery related to the Government's use of cell site simulator technology (often  
26



referred to as “Stingray,” one of the simulator models). *See* Govt. Response at 18. For the Government’s purposes, this is an unfortunate example to have chosen.

In *Rigmaiden*, the Government had used a cell site simulator to track and locate the defendant and his laptop. The court recognized that “[e]ven sensitive law enforcement information must be disclosed if it is needed for an effective defense.” 844 F. Supp. 2d at 988. The court then denied various motions for discovery related to the simulator because the Government had conceded facts that rendered the discovery moot (*see id.* at 995-96); the defendant had failed to claim that the discovery was relevant to potential issues at trial (*id.* at 990); or the Government had made a concrete showing that limited information (such as the identities of individual technicians who had operated the simulator) was privileged because disclosure of their identities could jeopardize their safety. *Id.* at 997. Moreover, the defendant had not agreed to any of the special protective measures that the Government has requested, and Mr. Michaud has agreed to, in this case.

The net result was that much of the technical information about cell site simulators that the defendant had requested was not disclosed for reasons not applicable in this case, and even so the trial court may have later regretted its decision. Since then, there has been a steady stream of revelations about the nature and capabilities of cell site simulators that were not disclosed to the court in *Rigmaiden*, and numerous other courts as well. For example, it is now known that devices of the type used in *Rigmaiden* not only collect location data about the target phone or laptop, but can also intercept the full content of phone calls and text messages; search and seize content from the phones and computers of innocent bystanders; and even manipulate a phone’s software to force it to act as a bugging device.<sup>4</sup> Just a few years after *Rigmaiden* was

---

<sup>4</sup> *See, e.g.,* Kim Zetter, *Turns Out Police Stingray Spy Tools Can Indeed Record Calls*, Wired.com. (October 28, 2015) (available at: <http://www.wired.com/2015/10/stingray-government-spy-tools-can-record-calls-new-documents-confirm/>); Adam Lynn, *Tacoma Police*

1 decided, over 2,000 cases in Maryland alone may be overturned because agents and  
2 prosecutors colluded to withhold discovery about cell site simulators.<sup>5</sup>

3 In short, the court in *Rigmaiden* rejected various discovery demands for reasons  
4 that do not apply here. More importantly, the case provides a stark illustration of the  
5 risks that are posed when the judiciary defers to governmental representations about  
6 whether discovery is relevant or whether it has already provided “sufficient” discovery.  
7 *See* Govt. Response (Dkt. 134) at 2.

8 **B. The Government Has Not Met Its Burden of Establishing that the**  
9 **Law Enforcement Privilege Applies.**

10 The Government claims that, even if the requested items are discoverable, the  
11 interests of law enforcement outweigh the defense’s interests. The Government  
12 concedes, however, that it must make some showing before the privilege even applies  
13 and before this Court gets into weighing the competing interests. Govt. Response at 14.  
14 Apart from invoking the privilege, however, it has made no concrete showing that the  
15 privilege applies or how law enforcement agents or pending investigations would be  
16 harmed by the discovery, especially in light of the special discovery protections that the  
17 Government requested and the defense is prepared to adopt.

18 More specifically, the Government’s basic assertions regarding the law  
19 enforcement privilege are not disputed. Substantively, the privilege can apply to  
20 Government investigative techniques, assuming that the Government makes an  
21 adequate showing of harm. Procedurally, if the Government can show that law  
22 enforcement interests would be harmed, the privilege involves a balancing of the  
23 competing defense and law enforcement interests. These principles are not disputed.

24 

---

 *Change How They Seek Permission to Use Cellphone Tracker*, The News Tribune, November  
25 15, 2014 (available at: [www.thenewstribune.com/news/local/crime/article25894096.html](http://www.thenewstribune.com/news/local/crime/article25894096.html)).

26 <sup>5</sup> Nicky Woolf, *2000 Cases May be Overturned Because Police Used Secret Stingray Surveillance*, The Guardian (Sept. 4, 2015) (available at: <http://www.theguardian.com/us-news/2015/sep/04/baltimore-cases-overturned-police-secret-stingray-surveillance>)

1 But the Government then reaches outside this Circuit to assert that there is a  
2 “pretty strong presumption against lifting the privilege.” Govt. Response at 16, citing  
3 *In re The City of New York*, 607 F.3d 923, 945 (2d Cir. 2010). This is a standard found  
4 nowhere in Ninth Circuit case law and it is inconsistent with the relevant Supreme  
5 Court authority. *See Roviato v. United States*, 353 U.S. 53, 60-61 (1957) (discussing  
6 the law enforcement privilege and withholding of an informant’s identity, and  
7 concluding that “[w]here the disclosure of an informant’s identity, or of the contents of  
8 his communication, is relevant and helpful to the defense of an accused, or is essential  
9 to a fair determination of a cause, *the privilege must give way*”) (emphasis added).

10 Further, *City of New York* was a *civil* case, quoting from another civil case,  
11 *Dellwood Farms, Inc. v. Cargill, Inc.*, 128 F.3d 1122, 1125 (7th Cir. 1997). The  
12 *Dellwood Farms* court stated that when civil parties seek to force the executive branch  
13 to divulge confidential information, the courts will be reluctant to be “thrust too deeply  
14 into the criminal investigative process.” *Id.* But the court emphasized that the plaintiffs  
15 were not criminal defendants and “thus have no definite legal right to the fruits of the  
16 FBI’s investigative endeavors conducted in confidence.” The court carefully  
17 distinguished the situation before it from one where, as here, there are “constitutional  
18 and other recognized legal rights of suspects and defendants.” *Id.*

19 In short, the Government’s civil, sister-circuit cases do not establish the law  
20 applicable to this criminal, Ninth Circuit case. Indeed, if anything, the *Dellwood Farms*  
21 case recognized that criminal defendants have discovery rights grounded in the right to  
22 a fair trial and effective representation that do not apply in the civil context.

23 The same applies to the Government’s attempt to erect a burden of showing “an  
24 authentic ‘necessity,’” or a “compelling need.” Govt. Response at 17 (citations  
25 omitted). As recently as last year, the Ninth Circuit repeated the standard set forth by  
26

1 the Supreme Court, which is simply that the discovery must be “relevant and helpful to  
2 the defense.” *In re Perez*, 749 F.3d 849, 855–56 (9th Cir. 2014).

3 The Government’s need for withholding the information (which it has merely  
4 stated, and not supported with any specifics) is further lessened because of the strict  
5 conditions under which defense review of the code would occur. As noted, the  
6 defense’s code expert has undergone security clearances and is willing to analyze the  
7 code at a government facility. The Government has not suggested that its previously  
8 proposed safeguards are now inadequate, nor has it in any way explained how such a  
9 closely protected and monitored review would compromise pending investigations. It  
10 has instead simply assumed that this Court would hear the Government’s claims ex  
11 parte, in camera, an issue to which the defense now turns.

### 12 **C. The Court Should Not Hold an Ex Parte, In Camera Hearing.**

13 The Government string cites cases in support of the unremarkable contention  
14 that ex parte, in camera hearings are *permissible* when the Government asserts the law  
15 enforcement privilege. Govt. Response at 15-16. Only six of these cases are from the  
16 Ninth Circuit. One of those six involved classified documents, where the court  
17 remarked that, outside of that context, “[e]x parte hearings are generally disfavored,”  
18 *United States v. Klimavicius-Viloria*, 144 F.3d 1249, 1261 (9th Cir. 1998). The code  
19 data in this case is not classified. All of the other Ninth Circuit cases involved  
20 confidential informants, where a court is faced with an all-or-nothing situation: The  
21 court either discloses the CI’s identity, creating a potential threat to the CI’s safety, or it  
22 holds an ex parte, in camera hearing.

23 Here, the Court is faced with a very different situation. The Government broadly  
24 asserts that disclosure of the computer code could somehow harm law enforcement.  
25 But the Government does not need to disclose the code in order to argue in favor of the  
26 law enforcement privilege. It could have detailed in its Response *why* disclosure of the

code would harm law enforcement, without yet revealing the code itself. It could even have presented those details in a sealed (but not ex parte) pleading, as it has done with so many other pleadings in this case. Instead, the Government has presented nothing to justify an ex parte hearing, beyond the fact that such hearings have at times been granted in other cases.

The Ninth Circuit has repeatedly stated that “absent some ‘compelling justification,’ ex parte communications will not be tolerated,” and that “ex parte proceedings are anathema in our system of justice.” *Guenther v. Comm’r*, 889 F.2d 882, 884 (9th Cir. 1989). The defense has previously briefed the Ninth Circuit’s view on ex parte proceedings and will not burden the Court by repeating that discussion here. *See* Reply to Govt. Response to Motion to Vacate and Response to Govt. Motion for In Camera Review (Dkt. 42) at 13-15. The Government has nonetheless chosen to provide no reason for this Court to believe an ex parte hearing is warranted. Under these facts, this Court should conclude that the Government has not demonstrated the “extraordinary circumstances” that might justify ex parte procedures and deny that request. *Wang v. United States*, 947 F.2d 1400, 1402 (9th Cir. 1991).

### III. CONCLUSION

The Court should grant the motion for discovery, without holding an ex parte, in camera hearing.

DATED this 8th day of February, 2016.

Respectfully submitted,

s/ *Colin Fieman*  
s/ *Alan Zarky*  
Attorneys for Jay Michaud

**CERTIFICATE OF SERVICE**

I hereby certify that on February 8, 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 to Colin Fieman  
Federal Public Defender Office