Sealed Documents

3:15-cr-05351-RJB USA v. Michaud

BOND

U.S. District Court

United States District Court for the Western District of Washington

Notice of Electronic Filing

The following transaction was entered by Fieman, Colin on 4/22/2016 at 3:18 PM PDT and filed on 4/22/2016

Case Name: USA v. Michaud
Case Number: 3:15-cr-05351-RJB
Filer: Dft No. 1 - Jay Michaud
Document Number: 178

Docket Text:
SEALED DOCUMENT ***Defense Consolidated Response to Government's Motion for Reconsideration, Renewed Motions for Ex Parte and In Camera Proceedings, and Defense Second Motion to Dismiss Indictment*** **by Jay Michaud, re [177] MOTION to Seal Document *Defense Consolidated Response to Gov't Mtn for Reconsideration*. (Attachments: # (1) Exhibit A, # (2) Exhibit B, # (3) Exhibit C)(Fieman, Colin)**

3:15-cr-05351-RJB-1 Notice has been electronically mailed to:

Andre M. Penalver andre.penalver@usdoj.gov, ecf-crm.usawaw@usdoj.gov, jennifer.shauberger@usdoj.gov, SPorter1@usa.doj.gov

Colin Fieman colin_fieman@fd.org, Carolynn_Calder@fd.org, Christine_Bowie@fd.org, Jessica_Cvitanovic@fd.org, WAW_ECF_notifications@fd.org

Keith Becker keith.becker@usdoj.gov

Linda R Sullivan linda_sullivan@fd.org, Carolynn_Cohn@fd.org, Christine_Bowie@fd.org, Jessica_Cvitanovic@fd.org, WAW_ECF_notifications@fd.org

Matthew Hampton Matthew.Hampton@usdoj.gov, dru.mercer@usdoj.gov, ecf-crm.usawaw@usdoj.gov, emily.miller@usdoj.gov

Matthew H Thomas matthew.h.thomas@usdoj.gov, Chantelle.Smith2@usdoj.gov, ECF-CRM.USAWAW@usdoj.gov, Ellaine.Wi@usdoj.gov, jennifer.biretz@usdoj.gov, Kelly.Shirkey@usdoj.gov, lisa.crabtree@usdoj.gov, Nichole.Barnes@usdoj.gov

Michael Dion michael.dion@usdoj.gov, ECF-CRM.USAWAW@usdoj.gov, Jackie.Masonic@usdoj.gov

Reginald E Jones reginald.jones4@usdoj.gov

3:15-cr-05351-RJB-1 Notice will not be electronically mailed to:

The following document(s) are associated with this transaction:

Document description: Main Document
Original filename:n/a
Electronic document Stamp:
[STAMP dcecfStamp_ID=1035929271 [Date=4/22/2016] [FileNumber=6113004-0
] [2ec2083bee52ee4414036add8913695ba0f93343a168e40f8bc6c02b9df8f4601c2
d1bfef0e970297413c61cd85e4c3227553b4a13b917b76834826b6410ae1c]]
Doc ument description: Exhibit A
Original filename:n/a
Electronic document Stamp:
[STAMP dcecfStamp_ID=1035929271 [Date=4/22/2016] [FileNumber=6113004-1
] [0f4a446192bc5ad7275329034da3250e7db39a36059c359f860e54c37a3303c368e
e1acecc834009c483e50d86af319bc0a8bb8341cca9f7539a1f258e99e3bd]]
Document description: Exhibit B
Original filename:n/a
Electronic document Stamp:
[STAMP dcecfStamp_ID=1035929271 [Date=4/22/2016] [FileNumber=6113004-2
] [2db9dd8f395b50511d7aa880baa1beebeb1923bda146b65c900cf36e9d9fd3839a4
197f375ff7bc2ccee7bbd7161ac6ebe819985a13a995a70325f257bcf78cc]]
Document description: Exhibit C
Original filename:n/a

Electronic document Stamp:
[STAMP dcecfStamp_ID=1035929271 [Date=4/22/2016] [FileNumber=6113004-3
] [2a16008c32412a36c1a55f708878bf8321470d175473454f2762da1d71523f679c4
d9e8c120704288874ee50fabd0db4718e21aa2ad8ea52c427fda6eff9cd67]]

JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	No. CR15-5351RJB CONSOLIDATED RESPONSE TO GOVERNMENT MOTION FOR RECONSIDERATION; RESPONSE TO MOTIONS FOR EX PARTE AND IN CAMERA PROCEEDINGS: AND SECOND DEFENSE MOTION TO DISMISS INDICTMENT **FILED UNDER SEAL**[1]

I. INTRODUCTION

Jay Michaud, through his attorneys Colin Fieman and Linda Sullivan, respectfully submits this Response to the Government's March 28, 2016, Motion for Reconsideration of the Court's February 17, 2016, Order for limited and secure disclosure of the NIT code that was used to hack into Mr. Michaud's computer and collect evidence that the Government will introduce at trial. The defense also replies to the Government's renewed motions for ex parte and in camera proceedings, and moves for dismissal of the indictment.

[1]The Government's filing of redacted and sealed versions of its motion is misguided, since it does not contain new or sensitive information that should be withheld from the public. The defense is nevertheless filing this response under seal, pending further guidance from the Court, since it quotes some of the statements that have been (inexplicably) redacted from the Government's public version of the motion. Mr. Michaud will also file a redacted version of this Response and follow with a motion to unseal all the discovery pleadings.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

The Government has now made plain that the FBI will not comply with the Court's discovery order. Motion for Reconsideration (Dkt. 165) at 3. The Government further acknowledges that "there may be consequences for this refusal." *Id.* Pursuant to the law discussed below, the consequences are straightforward: the prosecution must now choose between complying with the Court's discovery order and dismissing the case. If the Government does not meet its legal obligation to dismiss the case, Mr. Michaud respectfully moves the Court, pursuant to Fed. R. Crim. P. 16(d)(2)(D) and the Classified Information Procedures Act (CIPA) § 6, for dismissal.

This dilemma is one entirely of the Government's own making, and nothing in its Motion for Reconsideration or renewed requests for secret proceedings changes the analysis.

First, as summarized in the accompanying declaration (exh. B), all of the arguments presented in the Motion for Reconsideration were previously made by the Government (some several times over). The Court should therefore deny the Motion because such motions are "disfavored" and the Government does not allege that the Court's February 17, 2016, discovery order was based on "manifest error." L. Cr. R. 12(b)(10)(A). To the contrary, the Court's ruling was correct, consistent with the controlling case law, and grounded on Mr. Michaud's constitutional rights to effective assistance of counsel and a fair trial.

Further, the Government does not offer any "new facts or legal authority which could not have been brought to [the court's] attention earlier with reasonable diligence." *Id*. This deficiency is unaffected by the Government's renewed request to submit an ex parte pleading. While the Government acknowledges that it has previously moved to proceed ex parte in opposing discovery, it suggests that "it did not follow through on the request." Motion for Reconsideration at 2, lines 27-28. To the contrary, the Government briefed its prior motion for secret proceedings at some length. *See* Dkt.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

134 (Govt. Response to Motion to Compel) at 2, 13-16. The Court denied the request because the Government had not made any showing of need for such exceptional and highly disfavored proceedings. And the Government's motion now is merely a restatement of the same unelaborated claim that secret proceedings are necessary.

More importantly, the Government concedes that the actual discovery at issue is *not* classified. Motion for Reconsideration at 4. The Government also explains that its proposed ex parte pleading does not relate to the Court's core finding that the discovery is relevant and helpful to the defense. Instead, it would only address the "harms" that might result from disclosure and offers reasons why the FBI refuses to comply with the Court's order. Motion for Reconsideration at 3. As a result, the Government is making the novel and puzzling argument that, while "the information at the heart of the Court's discovery order remains unclassified," the Court should nevertheless allow ex parte proceedings simply "because the FBI has determined it cannot produce the information at issue." *Id.*

Finally, not only is the actual discovery at issue not classified, even if it were Congress has established procedures for protecting both legitimate national security interests and a defendant's constitutional rights to effective representation and a fair trial. *See* CIPA. As discussed in § III(B), *infra*, the Government has failed to meet the requirements of CIPA for submitting an ex parte pleading or proceeding in camera. As a result, the Court can and should summarily deny the renewed motions for secret proceedings.

In the final analysis, the Government cannot have it both ways -- on one hand charging a defendant with an offense that carries a five year mandatory minimum sentence, and on the other hand undermining his trial rights by deferring to the FBI's refusal to disclose evidence that the Court has found relevant and helpful. Having created this impasse, the Government must now address the consequences.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

II. ARGUMENT

A. THE DISCOVERY THAT THE COURT HAS ORDERED THE GOVERNMENT TO PRODUCE IS CRITICAL TO THE DEFENSE AND THE GOVERNMENT'S ARGUMENTS FOR VACATING THE ORDER ARE REPETITIVE AND STILL MERITLESS.

To begin, the Government does not claim that the Court's discovery order was based on "manifest error," and in fact it was manifestly correct. *See* L. Cr. R. 12(b)(10)(A). The Court found without hesitation that it is "satisfied that the defense has shown materiality [of the discovery] here to preparing the defense. I don't need to discuss that in depth, in my view. I think the papers speak for themselves." Exh. A (February 17, 2016 Hearing Transcript) at 17. Indeed, at the February 17 hearing, the Government appeared to concede the relevance of the NIT discovery, given (as one prosecutor stated) "how the government identified the defendant," "how it obtained the search warrant," and the fact that the FBI's NIT evidence "would no doubt be part of the narrative at trial." *Id*. at 13.

With its ruling, the Court also emphasized some broader concerns and fairness considerations. In particular, the Court noted that this case involves novel and important issues because "[t]he government hacked into a whole lot of computers on the strength of a very questionable warrant. . . [and] it comes 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. And the government should respond under seal and under the protective order, but the government should respond…." Exh. A at 18.

That response, after further delay, has come instead in the form of the Motion for Reconsideration. All of the facts and arguments in the Motion were set forth in the Government's multiple prior briefs and declarations. *See* Dkt. 123 (Govt. Response to Request for Expedited Hearing); Dkt. 134 (Govt. Response to Third Motion to Compel Discovery); Dkt. 156 (Govt. Surreply to Third Motion to Compel); Dkt. 157

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

(Declaration of Special Agent Daniel Alfin); Dkt. 160 (Declaration of Agent Robert Stone).

Rather than repeat in this brief all the points and authorities that the Court has already considered, the accompanying declaration identifies where in the record each of the claims in the Motion for Reconsideration has previously been addressed. *See* exh. B. And, as already noted, the Government acknowledges that the ex parte pleading it wants to submit offers no new facts related to the Court's finding that the NIT discovery is relevant and helpful. Motion for Reconsideration at 4. Instead, the proposed pleading relates only to purported "harms that could result from the disclosures." *Id*. at 3. Accordingly, the contents of the Government's proposed secret pleading (which it is precluded from submitting under CIPA anyway, *see* § III(B), *infra*) has no bearing on the Court's central finding that the discovery is material.

Further, the Court's focus at the February 17 hearing on the enhanced need for discovery in light of the Government's methods in this case is well-founded, given the sophistication of the FBI's surveillance technology and the evidence that it has misled the courts in other cases about that technology.

Coincidentally, just two days after the Government filed its Motion for Reconsideration, the Maryland Court of Special Appeals addressed at length the FBI's practice of concealing key information from defendants and courts. The court affirmed a suppression order in part because it found that local police and prosecutors had been instructed by the FBI not to disclose, *even if ordered to do so by a court*, the capabilities of the FBI's "Stingray" cell phone surveillance technology. *State v. Andrews*, 2016 WL 1254567 at *11-12 (Md. Ct. Spec. App. March 30, 2016). After initially hiding its use of "Stingray" entirely in warrant applications and discovery, agents and officers went on to mislead the courts about the fact that it captures more than just basic location information, as the FBI had claimed. As a result, thousands of

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

convictions in Maryland may be overturned. *See, e.g.*, Kim Zettter, *Turns Out Police Stingray Spy Tools Can Indeed Record Calls*, Wired.com. (October 28, 2015)[2]; Nicky Woolf, *2000 Cases May be Overturned Because Police Used Secret Stingray Surveillance*, The Guardian (Sept. 4, 2015).[3]

As the Maryland court observed, the FBI's obstruction of disclosure "from special order and/or warrant application through appellate review – prevents the court from exercising its fundamental duties under the constitution." 2016 WL 1254567 at *12. "[I]t is self-evident that the court must understand why and *how* [a] search was conducted," and "[t]he analytical framework requires analysis of the functionality of the surveillance device and the range of information potentially revealed by its use." *Id*. (emphasis in original). These conclusions mirror the conclusions reached by this Court at the February 17 hearing. *See* Exh. A at 18.

All of the Government's renewed arguments about the relevance of the discovery that was ordered by the Court should also be discounted in light of recent revelations about how the FBI conceals information about its NITs and other surveillance technology from federal prosecutors and even its own case agents.

As reported on April 20 in *USA Today*, FBI supervisors have ordered its Engineering Research Facility (ERF) and Technically Trained Agents (which are responsible for developing and deploying NITs and other "surveillance capabilities") to follow "Special Project Concealment" protocols for sharing information with Assistant U.S. Attorneys and case agents. Brad Heath, "FBI Warned Agents Not to Share Tech

[2] Available at: http://www.wired.com/2015/10/stingray-government-spy-tools-can-record-calls-new-documents-confirm/

[3] Available at: http://www.theguardian.com/us-news/2015/sep/04/baltimore-cases-overturned-police-secret-stingray-surveillance

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Secrets with Prosecutors," *USA Today*, April 20, 2016.[4] These protocols require the FBI's technical specialists to withhold information about NITs and other "techniques" from prosecutors and case agents so that they are unable to share information during discovery or cross-examination. *See* exh. C (two of the internal FBI emails referenced in *USA Today*). As a result, all of the representations in the Motion for Reconsideration (and the accompanying declaration of case agent Daniel Alfin) about what the discovery would show and its relevance to pre-trial issues and potential defenses are not only repetitive but inherently unreliable.

It is with these types of machinations in mind that the Maryland Court of Appeals went on in *Andrews* to quote the great Washingtonian and Supreme Court Justice William O. Douglas, who presciently observed many years ago that "[w]e are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government. The aggressive breaches of privacy by the Government increase by geometric proportions. Wiretapping and 'bugging' run rampant, without effective judicial or legislative control." *Andrews* at *10, quoting *Osborn v. United States*, 385 U.S. 323, 340 (1966) (Douglas, J., dissenting). "Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite unlike any we have seen — a society in which government may intrude into the secret regions of man's life at will." *Osborn*, 385 U.S. at 341.

More basically, and regardless of the Government's credibility when it insists that the defenses that Mr. Michaud is seeking to develop are "baseless" (Motion for Reconsideration at 9), the Ninth Circuit has clearly held "that [a] party seeking to impeach the reliability of computer evidence should have sufficient opportunity to

[4] Available at: http://www.usatoday.com/story/news/2016/04/20/fbi-memos-surveillance-secrecy/83280968/

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

ascertain by pretrial discovery whether both the machine and those who supply it with data input and information have performed their tasks accurately." *United States v. Budziak*, 697 F.3d 1105, 1112 (9th Cir. 2012) (citation omitted).

Budziak also involved a child pornography prosecution in which the defendant sought discovery of software that the FBI had used to search for digital files. *Id*. at 1108. Like the instant case, the FBI asserted a law enforcement privilege for the software. The Ninth Circuit nonetheless held that "access to the . . . software was crucial to Budziak's ability to assess the program and the testimony of the FBI agents who used it to build the case against him." *Id.* at 1112.

Notably, just as in this case, the Government argued in *Budziak* that it had disclosed computer logs and other materials that were "sufficient" for the defense; disputed the defense expert's declaration that examination of the software would be helpful; and insisted that Budziak "would not uncover any helpful information through discovery of the software." *Id*. at 1112; *compare* Second Declaration of Special Agent Alfin, Dkt. 166-2 at 2 ("Disclosure of the 'exploit' would do nothing to shed light on whether the government exceeded the scope of the NIT warrant.").

Likewise, in its Motion for Reconsideration, the Government disputes and disparages the defense's proffers and experts. *See, inter alia.*, Motion for Reconsideration at 8 (characterizing Mr. Michaud's potential pre-trial motions and defenses as "speculation"). But these objections are unavailing even if they could be taken at face value. The Ninth Circuit ultimately reversed the conviction in *Budziak* because a "district court should not merely defer to government assertions that discovery would be fruitless," and "criminal defendants should not have to rely solely on the government's word that further discovery is unnecessary." *Id.* at 1113; *see also United States v. Johnson*, 459 F.3d 990, 993 (9th Cir. 2006) (juries, not prosecutors or judges, must decide the viability of potential defenses, and a defendant is entitled to

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

present his theories of defense "even if his evidence is weak, insufficient, inconsistent, or of doubtful credibility") (citation omitted).

The Government's refusal to comply with the discovery order is all the more untenable given the exceptional technical complexities that are involved with the Tor network and the FBI's use of sophisticated hacking "techniques." Just a few weeks ago, Seattle police raided the home of two people who use the Tor network, based on an allegation that their IP addresses had been linked to child pornography, when in fact illicit traffic had merely passed through their connection to the network. Martin Kaste, "When a Dark Web Volunteer Gets Raided by the Police," NPR.org (April 4, 2016).[5]

Similarly, a few years ago independent experts determined that NIT-type malware used by German law enforcement (despite a law prohibiting them from using malware) had left target computers vulnerable to "Trojan" viruses. These viruses, among other problems, allow third parties to remotely store child pornography on infected computers. *See* "Chaos Computer Club Analyzes Government Malware," available at: http://www.ccc.de/en/updates/2011/staatstrojaner ("We were surprised and shocked by the lack of even elementary security in the [police] code. Any attacker could assume control of a computer infiltrated by the German law enforcement authorities.").

The German analysis also revealed that much of the data collected by the police had been corrupted and was unreliable. *Id.* Determining the reliability of the Government's data "identifiers" and digital "chain of custody" are just two of the issues that the defense identified as important in this case and that can only be addressed through review of the discovery that the Court has already ordered the Government to produce. *See* Dkt. 115-A (Declaration of Vlad Tsyrklevitch) at ¶ 6.

[5] Available at: http://ideastations.org/radio/all-things-considered/npr-472992023-when-dark-web-volunteer-gets-raided-police

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Notably, these types of vulnerability and data verifications issues were central to a child pornography case that defense counsel tried before Judge Ronald Leighton.[6] Despite the Government's insistence that the defense's focus on potential vulnerabilities was "baseless" and could not account for the pornography found on the defendant's digital storage devices, the jury concluded otherwise and acquitted the defendant of five counts of receipt and possession of child pornography. *See also* CBS News, "Viruses Frame PC Owners for Child Porn," November 9, 2009 ("Of all the sinister things that Internet viruses can do, this might be the worst: They can make you an unsuspecting collector of child pornography…. Pedophiles can exploit virus-infected PCs to remotely store and view their stash without fear they'll get caught.");[7] Jo Deahl, "Websites Servers Hacked to Host Child Abuse Images," BBC News, August 5, 2013 (reporting on how malware created files on business computers to store images and how visitors to legal pornography sites had been redirected to illegal material.).[8]

To make matters worse, the Government has demonstrated that it will use its nondisclosure as both a sword and a shield if the defense pursues similar issues at trial. As noted in earlier briefing, the Government assured the Court before the January suppression hearing that it had already provided sufficient code discovery for the defense to litigate the pending suppression motions. *See* Dkt. 123. Yet, during the suppression hearing itself, the Government objected several times to the testimony of Dr. Christopher Soghoian about how NITs can compromise computer data and security settings, on the ground that his opinion "isn't based on any analysis of a network

---

[6] In order not to publicly reveal the nature of serious charges against a former client, counsel will not identify the case here but can separately inform opposing counsel and the Court of the case name and number upon request.

[7] Available at: http://www.cbsnews.com/news/viruses-frame-pc-owners-for-child-porn/

[8] Available at: http://www.bbc.com/news/uk-23551290

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

investigative technique in this case." January 22, 2016 Hearing Transcript at 102; *see also id.* at 105. Given this preview of the prosecution's strategy for dealing with defense experts, there is good cause to believe that the defense will be at a significant disadvantage at trial if the Court reverses its discovery order.

Finally, there is a striking inconsistency between the FBI's refusal to comply with the Court's order here and the position that the FBI took in the recent litigation against Apple. In the San Bernardino shootings case, the FBI minimized Apple's concern that forcing it to create custom code capable of bypassing the iPhone's security features would result in security risks for millions of customers. For example, in its motion to compel Apple, the Government stated that "to the extent that Apple has concerns about turning over software to the government," the use of a secure location to load the codes "eliminates any danger that the software required by the Order would go into the 'wrong hands[.]'" *In the Matter of the Search of an Apple i-Phone*, CM16-10 (E.D. Ca.), Dkt. 1 at 25.

Yet, in this case, the FBI is refusing to allow a defense expert with security clearance to review the NIT data, based on a broad assertion "that the risks of disclosure far outweigh the consequences for failure to comply with the order." Motion for Reconsideration at 3. The FBI has staked out this position despite the fact that the discovery sought by the defense already exists and is readily accessible (while the FBI wanted to force Apple to create new code), and the defense has offered to review the discovery at a secure facility (like the one that the Government proposed in the Apple litigation).

Given these facts, the FBI's position that it will not comply with the Court's order under any circumstances is tenable only if it is indeed prepared to accept "the consequences for failure to comply." The consequence (as discussed in § C below) should be dismissal of the indictment.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

B. THE GOVERNMENT'S RENEWED MOTIONS FOR EX PARTE AND IN CAMERA PROCEEDINGS SHOULD BE DENIED BECAUSE IT HAS NOT MET EVEN THE THRESHOLD REQUIREMENTS OF CIPA.

1. The Government's Motion to Submit an Ex Parte Pleading.

The Government seeks to bolster its Motion for Reconsideration with renewed requests for ex parte and in camera proceedings. The Government alleges that secret proceedings are needed because it wants to present "classified information" about how potential harms may arise from limited disclosure of the non-classified NIT discovery. Motion for Reconsideration at 2. The Government's request should be denied because, among other reasons, it has not met the requirements for secret proceedings under the Classified Information Procedures Act, 18 U.S.C. app. 3 (2000).

To begin, the Government has made no effort to explain how the classified information it wants to submit could have any meaningful bearing on the Court's discovery order. As noted, the NIT discovery ordered by the Court is not classified. *See* Motion for Reconsideration at 4. The Government is therefore making a convoluted request for ex parte proceedings so that it can submit classified information about why it will not disclose *un*classified information. Defense counsel has been unable to find any case where a court has allowed ex parte proceedings for such tangential information.

Moreover, despite the numerous pleadings and declarations that the Government filed prior to the Court's discovery order, it has never previously claimed that anything related to the discovery issues is classified. Under L. Cr. R 12(b)(10)(A), a court should "ordinarily deny" motions for reconsideration if the motion relies on facts that could have been "brought to its attention earlier with reasonable diligence."

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Further, and regardless of the questionable timing of the Government's classification claim, its motions for secret proceedings are effectively foreclosed by CIPA. In *United States v. Sedaghaty*, 728 F.3d 885 (9th Cir. 2013), the Ninth Court explained the process the Government is required to follow under CIPA when it wants to rely on classified information.

As a general matter, any effort by the Government to withhold information from a defendant based on a claim of secrecy must be considered in light of "the Constitution's guarantee that all criminal defendants must have 'a meaningful opportunity to present a complete defense.'" *Id*. at 906, *quoting Holmes v. Carolina*, 547 U.S. 319, 324 (2006). "Indeed, the 'need to develop all relevant facts in the adversary system is both fundamental and comprehensive.'" *Id., quoting United States v. Nixon*, 418 U.S. 683, 709 (1974).

With these principles in mind, Congress enacted CIPA to help ensure that intelligence agencies (and law enforcement agencies using classified information or claiming national security interests) "are subject to the rule of law and to help strengthen the enforcement of laws designed to protect both national security and civil liberties." *Id*. at 903, quoting S. Rep. No. 96-823 at 3 (1980).

The Ninth Circuit further explained that "CIPA does not expand or restrict established principles of discovery and does not have a substantive impact on the admissibility of evidence." *Sedaghaty*, 728 F.3d at 904 (citation omitted). Instead, when considering a motion to withhold classified information from a defendant, "a district court must first determine whether, pursuant to the Federal Rules of Criminal Procedure, statute, or the common law, the information at issue is discoverable at all." *Id.* This Court has, of course, already decided that the NIT data is not only discoverable but important to the defense, and by extension any pleading the Government wants to submit to challenge the Court's decision should also be discoverable. *See also Budziak,*

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

supra; *United States v. Libby*, 429 F. Supp. 2d 1, 7 (D.D.C. 2006) ("[CIPA] creates no new rights or limits on discovery of a specific area of classified information" and "it contemplates an application of the general law of discovery in criminal cases to the classified information") (citation omitted).

Once a court has determined that information is discoverable, it "must next determine whether the government has made a formal claim of the state secrets privilege," thereby establishing that sharing the information with the defense could pose a national security risk. *Sedaghaty*, 728 F.3d 904. This claim must be "lodged by the head of the department which has actual control over the matter, after actual personal consideration by that officer." *Id*. (quotation marks and citation omitted). The certification requirement serves to ensure that a classification claim is not made for tactical purposes or for purposes of delay. *Cf. United States* v. *Stewart*, 590 F.3d 93, 130 (2d Cir. 2009) (the purpose of CIPA is to protect sensitive national security information, not to impede a defendant's fair trial rights).

No such certification has been filed in this case, and this failure alone should end the matter. *See United States v. Turi*, 103 F. Supp. 3d 1068, 1069 (D. Ariz. 2015) (CIPA and Ninth Circuit precedent require the head of the government agency that has control over the classified information to file a formal state secrets claim with the court before seeking ex parte proceedings). The Government's omission is all the more problematic given that it is asking to submit an ex parte pleading in the context of a motion for reconsideration. While L. Cr. R. 12(b)(10) requires the Government to show that it could not previously have offered "new facts" in support of reconsideration with "reasonable diligence," in this case the prosecution still has not taken the preliminary steps needed to even request ex parte consideration of any classified information.

Moreover, even if the Government had met the certification requirement, the road to secret proceedings just gets steeper. Specifically, if the Government had filed a

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

certification, the Court would then be empowered under CIPA § 4 "to determine the terms of discovery" for any classified information. *Sedaghaty*, 728 F.3d at 904. To that end, CIPA § 3 expressly authorizes protective orders for disclosure of classified information, something the defense has not objected to and the Court has already approved for the code discovery. The Government is therefore hard pressed to explain why it should be allowed to proceed ex parte now when the very discovery at issue is not classified and is already subject to a protective order that, if necessary, could be made even more restrictive to cover any relevant classified information.

While CIPA also authorizes ex parte procedures as part of the discovery process, they are appropriate only under exceptional circumstances that do not apply here. Ex parte proceedings both generally and under CIPA are highly disfavored. As the Ninth Circuit has stated, they "are anathema in our system of justice." *Guenther v. Commissioner of Internal Revenue*, 889 F.2d 882, 884 (9th Cir. 1989); *see also, e.g., Detroit Free Press v. Ashcroft*, 303 F.3d 681, 683 (6th Cir. 2002) ("Democracies die behind closed doors."). This is because, as the Ninth Circuit has observed in the analogous context of a secret evidence case, "[o]ne would be hard pressed to design a procedure more likely to result in erroneous deprivations . . . . [T]he very foundation of the adversary process assumes that use of undisclosed information will violate due process because of the risk of error." *American-Arab Anti-Discrimination Committee v. Reno*, 70 F.3d 1045, 1969 (9th Cir. 1995) (internal quotation marks and citation omitted).

Indeed, by their very nature and regardless of how conscientious a trial judge may be, ex parte proceedings impair the integrity of the adversary process and the criminal justice system. As the Supreme Court has stressed, "'[f]airness can rarely be obtained by secret, one-sided determination of facts decisive of rights . . . . No better instrument has been devised for arriving at truth than to give a person in jeopardy of

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

serious loss notice of the case against him and opportunity to meet it.'" *United States* v. *James Daniel Good Real Prop.*, 510 U.S. 43, 55 (1993) (ellipsis in original, citation omitted).

And, as the Seventh Circuit has observed, "[i]t is a matter of conjecture whether the court performs any real judicial function when it reviews classified documents in camera. Without the illumination provided by adversarial challenge and with no expertness in the field of national security, the court has no basis on which to test the accuracy of the government's claims." *Stein v. Dept. of Justice*, 662 F.2d 1245, 1254 (7th Cir. 1981); *see also Dennis v. United States*, 384 U.S. 855, 875 (1966) ("In our adversary system, it is enough for judges to judge. The determination of what may be useful to the defense can properly and effectively be made only by an advocate.").

With these principles in mind, Congress determined when enacting CIPA that "the defendant should not stand in a worse position, because of the fact that classified information is involved, than he would without the Act." *See* S. Rep. No. 96-823 at 9 (1980). CIPA therefore not only requires the Government to file a certification before trying to rely on classified information, it further requires it to make a "sufficient showing" as to why a protective order is inadequate and classified information cannot be made available to the defendant pursuant to such an order. CIPA § 4. And then, even if the Government makes this showing, an appropriate next step (even in terrorism cases) would be to allow defense counsel to seek a security clearance or for the Court to appoint an attorney with clearance to review and challenge classified pleadings on the defendant's behalf. *Cf. In re Terrorist Bombings of United States Embassies in East Africa*, 552 F.3d 93, 118 (2d Cir. 2008).[9]

[9] It should go without saying that defense counsel will abide by the terms of any protective order issued by this Court prohibiting the defense from sharing details about the "potential harms" that might be offered in an additional pleading. But the defense is prepared to accept any other measures, including the appointment of additional counsel with security clearance, that the Court deems appropriate to move forward.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

In this case, however, the Government has made little or no showing as to why the Court should allow a secret pleading. *Wang v. United States*, 947 F.2d 1400, 1402 (9th Cir. 1991) (requests for ex parte proceedings should be denied if the movant has not demonstrated "extraordinary circumstances" that justify such procedures). While the Government may not want to disclose the *details* of the pleading that it claims is relevant, that does not prevent it from offering at least *general reasons* why allowing defense counsel to see it could be harmful, such as alleging that sharing the pleading would place agents or informants at risk. *See Roviaro v. United States*, 353 U.S. 53, 60-61 (1957) (ultimately holding that, with informant information, "[a] further limitation on the applicability of [a law enforcement privilege] arises from the fundamental requirements of fairness. Where the disclosure of an informer's identity . . . is relevant and helpful to the defense of an accused, or is essential to a fair determination of a cause, the privilege must give way").

Given that the code discovery itself is not classified, it is already difficult to fathom how any secondary information about potential harms that might arise from limited disclosure of unclassified information is so sensitive that the Court must exclude defense counsel from seeing it.

This is especially true given all the public information that is already available about the Government's use of malware and NITs. *See* NSA "Egotistical Giraffe" Documents (detailed NSA documents describing the NIT "native Firefox exploit" that is used to target Tor users)[10]; Matt Apuzzo, "F.B.I. Used Hacking Software Decade Before iPhone Fight," *The New York Times*, April 13, 2016 (describing the FBI's use of NIT-type malware to target animal rights activists);[11] Craig Timberg and Ellen

[10] Available at: http://www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document

[11] Available at: http://www.nytimes.com/2016/04/14/technology/fbi-tried-to-defeat-encryption-10-years-ago-files-show.html

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Nakashima, "FBI's search for 'Mo,' Suspect in Bomb Threats, Highlights Use of Malware for Surveillance," *The Washington Post*, December 6, 2013 (Reporting in detail on the FBI's NITs, including their ability to "covertly download files, photographs and stored e-mails, or even gather real-time images by activating cameras connected to computers").[12]

In fact, FBI Director James Comey recently boasted during Congressional testimony about his agency's ability to identify people who use the Tor network. Speaking about people who visit child pornography sites in particular, Director Comey testified that "[t]hey'll use the onion router to hide their communications. They think that if they go to the dark web … that they can hide from us. They're kidding themselves, because of the effort that's been put in by all of us in the government over the last five years or so, that they are out of our view." Dan Froomkin, "FBI Director Claims Tor and the 'Dark Web' Won't let Criminals Hide from his Agents," *The Intercept*, September 10, 2015 (ellipsis in original).[13] As a result, Tor activists and Mozilla (which produces the Firefox browser used by Tor) are already working on patching the Tor vulnerabilities that were exploited by the FBI. *See* Joseph Cox, "The FBI May be Sitting on a Firefox Vulnerability," *Motherboard*, April 13, 2016 (noting that, while the "exploits" used by the FBI are helpful for catching some criminals, they are also exposing millions of law-abiding people to hacking by other criminals and foreign governments).[14]

---

[12] Available at: : https://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html.

[13] Available at: https://theintercept.com/2015/09/10/comey-asserts-tors-dark-web-longer-dark-fbi/

[14] Available at: http://motherboard.vice.com/read/the-fbi-may-be-sitting-on-a-firefox-vulnerability

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

In other words, the cat is long out of the bag when it comes to the FBI's use of NITs and what those NITs do. With all this public information (much of it from the Government itself, when it suits its purposes), only the most clueless of criminals or potential terrorists would continue to believe that their activities on Tor remain anonymous. It is therefore incumbent on the Government to explain how any pleading that merely summarizes "the harms that could result from the disclosures ordered" is so sensitive that the Court must exclude defense counsel and resort to secret proceedings. *See* Motion for Reconsideration at 3.

In sum, the Government has no grounds for withholding the NIT discovery itself under CIPA because it is not classified and the defense is not seeking to share the discovery or disclose it in open court.

Further, the Government has not met the certification requirement for asserting a state secrets claim. This omission, in combination with the Government's failure to raise this "classified information" claim in a timely manner, not only casts doubt on the validity of its request for secret proceedings, but precludes an ex parte submission.

And, finally, the Government has made no showing as to why sealing its proposed pleading or submitting it under a protective order (perhaps limiting review to one of Mr. Michaud's attorneys) is insufficient. *See also, generally*, *United States* v. *Abuhamra*, 389 F.3d 309, 322 (2d Cir. 2004) ("Particularly where liberty is at stake, due process demands that the individual and the government each be afforded the opportunity not only to advance their respective positions but to correct or contradict arguments or evidence offered by the other.").

2. The Government's Motion for an In Camera Hearing.

In addition to its motion to file an ex parte pleading, the Government has also moved for an in camera hearing. Motion for Reconsideration at 2. This should also be

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

denied for two reasons. First, like its request for an ex parte submission, the Government has made no showing as to why an in camera hearing is needed.

Second, the Government has again ignored the requirements of CIPA, which provides that the Government can seek an in camera hearing to determine "the use, relevance and admissibility of classified information" only "if the Attorney General certifies to the Court. . . that a public proceeding may result in the disclosure of classified information." CIPA § 6(a); *see also* Motion for Reconsideration at 3 (where, despite the lack of certification, the Government maintains that "the conclusion reached by those tasked with making these decisions is that the risks of disclosure far outweigh the consequences for failure to comply with the Order"). This requirement is separate from the certification requirement for ex parte pleadings, and serves the important purpose of preventing the Government from requesting secret hearings absent a claim of exceptional circumstances endorsed by the Attorney General herself. No certification has been filed in this case, and this fact alone warrants denial of the Government's motion.

In light of all these facts and omissions, and the applicable law, the Court should find that the Government's repeated invocation of "law enforcement exemption" and "national security" is just as insufficient now as it was when the Court denied the Government's previous requests for secret proceedings.

C. THE GOVERNMENT IS REQUIRED TO CHOOSE BETWEEN COMPLYING WITH THE COURT'S ORDER OR DISMISSING THE INDICTMENT, AND IF IT SIMPLY MAINTAINS ITS REFUSAL TO COMPLY THE COURT ITSELF SHOULD DISMISS.

In its Motion for Reconsideration, "[t]he United States recognizes that there may be consequences for [its] refusal" to comply with the Court's discovery order. Motion

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

for Reconsideration at 3. That consequence should be dismissal of the indictment against Mr. Michaud.

In this case, the choice between disclosure and dismissal is one that the Government has forced upon itself (or, at least, the FBI has forced on the prosecutors). The Government has had ample opportunity to be heard on the discovery issues (the defense made its initial discovery request for the NIT code eight months ago); the prosecution has filed multiple and repetitive pleadings challenging discovery; it has raised the specter of national security without so much as attempting to follow the procedures Congress has established for dealing with such matters in a criminal case; and it has flatly refused to adopt additional security measures for discovery that would address any legitimate security concerns.

Pursuant to CIPA § 6(e)(2), once the Government has properly asserted a state secrets claim (which it has not done in this case), and the Court has determined that the information at issue is material to the defense and imposed appropriate discovery limitations (which the Court has done with its protective order), "it falls to the government to elect between permitting the disclosure of that information or the sanctions the court may impose, including dismissal of the charges against the defendant." Edward Liu and Todd Garvey, "Protecting Classified Information and the Rights of Criminal Defendants," Congressional Research Service 7-5700 at 5, April 2, 2012.[15] The dismissal provision of CIPA is consistent with Fed. R. Crim. 16(d)(2)(D), which provides that, if a party fails to comply with a discovery order, the court may "enter any other order that is just under the circumstances." *See also Roviaro*, 353 U.S. at 60 (When a trial court has found that discovery "is relevant and helpful to the

[15] Available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0ahUKEwjS9O_Hk5zMAhVS7mMKHWxsDSgQFggdMAA&url=https%3A%2F%2Fwww.fas.org%2Fsgp%2Fcrs%2Fsecrecy%2FR41742.pdf&usg=AFQjCNGZTr6qpR2wf-EXeFzBu_r3YAj8DQ&sig2=xGZz67BQ-rSeQWjxbahOrQ

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

defense" and the Government persists in withholding it, the court may "dismiss the action").

Given that the actual discovery ordered by the Court is not even classified, the FBI's refusal to comply with the Court's order is particularly egregious. Indeed, the Court has already warned the Government that it would be treading on thin ice if it persisted in opposing discovery, when it told prosecutors in February that "you can either produce [the discovery] or move to dismiss." Exh. A at 19. The Court also reminded the Government at the time that it had the option of appealing its discovery order on an interlocutory basis, an option that it has elected not to pursue. *Id*. at 20.

This is not the first time that the FBI's refusal to provide discovery has forced prosecutors to choose between compliance with a discovery order and dismissal. For example, in connection with the "Stingray" cases discussed above, the FBI in fact ordered local prosecutors to dismiss cases or reduce felonies to minor charges rather than comply with discovery orders. *See Andrews*, 2016 WL 1254567 at *11 (citing the Baltimore State Attorney's agreement that it "will, at the request of the FBI, seek dismissal" rather than disclose information about the technology); Ellen Nakashima, "Secrecy Around Police Surveillance Equipment Proves a Case's Undoing," *The Washington Post*, February 22, 2015 (FBI required Florida prosecutors to reduce armed robbery charges to second degree misdemeanor rather than comply with discovery order);[16] Justin Fenton, "Judge Threatens Detective with Contempt for Declining to Reveal Cellphone Tracking Methods," *The Baltimore Sun*, November 17, 2014

[16] Available at: https://www.washingtonpost.com/world/national-security/secrecy-around-police-surveillance-equipment-proves-a-cases-undoing/2015/02/22/ce72308a-b7ac-11e4-aa05-1ce812b3fdd2_story.html

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

(prosecutors withdrew key evidence in a robbery case rather than comply with discovery order).[17]

Even assuming that the Government has good faith reasons in this case for refusing to comply with the Court's order, the Supreme Court has recognized that electing between discovery and dismissing charges is a choice that prosecutors must sometimes make. "The rationale of the criminal cases is that, since the Government which prosecutes an accused also has the duty to see that justice is done, it is unconscionable to allow it to undertake prosecution and then invoke its governmental privileges to deprive the accused of anything which might be material to his defense." *Jencks v. United States*, 353 U.S. 657, 671 (1957) (quotation and citation omitted).[18]

The Court therefore held "that the criminal action must be dismissed when the Government, on the ground of privilege, elects not to comply with an order to produce[.]" *Id.* at 672. "The burden is the Government's, not to be shifted to the trial judge, to decide whether the public prejudice of allowing the [alleged] crime to go unpunished is greater than that attendant upon the possible disclosure of state secrets and other confidential information in the Government's possession." *Id.* In other words, once a trial court has decided that discovery is material to the defense, it is not the court's role to further weigh the need for disclosure against the potential harms of that disclosure. Rather, the Government must decide between complying with the discovery order and dismissing its charges.

Here, the Government has already signaled its decision. It has stated that the FBI will not comply with the Court's discovery order under any circumstances, and it

---

[17] Available at: http://www.baltimoresun.com/news/maryland/baltimore-city/bs-md-ci-stingray-officer-contempt-20141117-story.html

[18] Although the timing of the specific discovery at issue in *Jencks* has been modified by statute, 18 U.S.C. § 3500, the basic principles still apply.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

has acknowledged that this refusal entails consequences. Motion for Reconsideration at 3. All that remains, if the Government will not make the responsible choice of filing a motion to dismiss itself, is for the Court to grant Mr. Michaud's motion for dismissal.[19]

III. SUMMARY AND CONCLUSION

The Government's efforts to extend its law enforcement powers in "Operation Pacifier" and avoid further review of its actions is seemingly boundless.

First, as this Court found, the Government violated Rule 41 and obtained a warrant that is unprecedented in its scope, targeting over 100,000 people. While the Court denied Mr. Michaud's suppression motion, it has observed that the warrant was at best "questionable" and survived based on "a narrow ruling" on admissibility. Exh. A at 18.[20]

Next, the Government used its malware through the unprecedented means of actively distributing tens of thousands of child pornography pictures and videos. These tactics are particularly troubling because the FBI had no investigatory need to re-victimize minors in order to identify the visitors that were signing into its pornography site.

Worse yet, the FBI boosted the number of visitors to Playpen from approximately 11,000 per week prior to the site's seizure to over 50,000 per week while it was under FBI control. *See* Dkt. 109 (Govt. Response to Order Compelling

---

[19] There are also no significant countervailing public safety concerns that, while not a factor in determining the motion for dismissal under the applicable law, might still concern the Court. Mr. Michaud has been on pre-trial supervision for almost a year and he has been in complete compliance with the onerous conditions of his release. He has had a favorable psycho-sexual evaluation and passed a polygraph test. *See* Dkt. 127-1. He is also 63 years old, retired, has no criminal history, and the Government has made no allegations of "hands on" contact with minors in connection with the Internet offenses that have been charged.

[20] On April 20, the Hon. William G. Young of the District of Massachusetts issued an order suppressing all evidence in a Playpen case, finding that the Virginia NIT warrant was "void ab initio" and that the FBI had not acted in good faith reliance on it. *United States v. Levin*, CR15-10271WGY, Dkt. 69.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Discovery) at 4; Dkt. 41, exh. C at ¶ 19. The only apparent explanation for this immediate and explosive increase in the number of visitors to Playpen is that the FBI actively redirected people to its site. Alternatively, the FBI attracted thousands of new and likely unwitting visitors to its site by maintaining a home page for it that was different from the one described in the NIT warrant application and devoid of lascivious images or any other obvious indication that the site contained child pornography. While there might be other and more innocent explanations for the troubling Playpen visitor numbers, the Government has offered none.

And now, as the defense seeks to review the full scope of the Government's actions and prepare for trial, the FBI has announced that it will not comply with the Court's discovery order, regardless of (1) the fact that the discovery at issue is not classified; (2) the security procedures available for sensitive materials under CIPA; and (3) defense counsel's repeated offers to accommodate any legitimate security concerns with an enhanced protective order.

Taking the totality of these facts and circumstances into account, as well as the applicable law, the Court should deny the Government's Motion for Reconsideration; deny the Government's motions for ex parte and in camera proceedings; and grant the defense's motion for dismissal of the indictment.

DATED this 22nd day of April, 2016.

Respectfully submitted,

s/ *Colin Fieman*
s/ *Linda Sullivan*
Attorneys for Jay Michaud

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

CERTIFICATE OF SERVICE

I hereby certify that on April 22nd, 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.

I further certify that emailed a copy of the foregoing sealed document and exhibits to the registered parties.

s/ *Amy Strickling, Paralegal*
Federal Public Defender Office

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, vs. JAY MICHAUD, Defendant.	Docket No. CR15-5351RJB Tacoma, Washington February 17, 2016

TRANSCRIPT OF MOTION HEARING
BEFORE THE HONORABLE ROBERT J. BRYAN
SENIOR UNITED STATES DISTRICT COURT JUDGE

APPEARANCES:

For the Plaintiff:
MATTHEW HAMPTON
Assistant United States Attorney
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402

KEITH BECKER
U.S. Department of Justice
1400 New York Avenue NW, 6th Floor
Washington, DC 20530

For the Defendant:
COLIN FIEMAN
LINDA SULLIVAN
Office of the Public Defender
1331 Broadway, Suite 400
Tacoma, Washington 98402

Court Reporter:
Teri Hendrix
Union Station Courthouse, Rm 3130
1717 Pacific Avenue
Tacoma, Washington 98402
(253) 882-3831

Proceedings recorded by mechanical stenography, transcript produced by Reporter on computer.

Exhibit A-001

Wednesday, February 17, 2016 - 9:30 a.m.

(Defendant present.)

THE CLERK: All rise. This United States District Court is now in session, the Honorable Robert J. Bryan presiding.

THE COURT: Please be seated. Good morning.

This is United States versus Jay Michaud, No. 15-5351. It is set this morning for hearing on the defendant's third motion to compel. The defendant is present with his attorneys, Ms. Sullivan and Mr. Fieman. And Mr. Becker and Mr. Hampton are here for the government.

The first order of business is a surreply. The government has filed a motion for leave to file a surreply. I gather the defense objected.

MR. FIEMAN: Yes, Your Honor. You probably already read it already and we are prepared to address it, so we can note our objection.

THE COURT: I think it is proper to allow it. So I have signed the order authorizing that.

Now, in preparation for this proceeding I have read your briefing, all of it twice, and reviewed some things in the file. I guess this goes back to the hearing that we had on the 14th of December where I thought this issue was resolved at that time.

Mr. Fieman indicated that the government had notified them

that the government was in fact willing to turn over the NIT code. The government, in the pleading, filed on the 5th of January, said the government has agreed to provide to the defense and its expert certain information related to a court-authorized Network Investigative Technique.

I guess I take it from those two things that you didn't in fact have an agreement to provide all of the code. Is that what leads to this motion to compel?

MR. FIEMAN: Your Honor, I thought we had an agreement, but apparently we did not have a meeting of the minds. I don't want to second-guess what the government's understanding was, but I would note I did put on the record at that hearing our understanding, and there was no qualification or comment from the government that we were only going to be getting a fraction of the information. So I was surprised by the government's position, but they staked it out and I guess we need to move forward.

THE COURT: Yes, okay.

Well, it is your motion, Mr. Fieman, so anything you want to add to your briefing.

MR. FIEMAN: Thank you, Your Honor.

So Your Honor, I will be brief, but I do want to make a few points, in particular, in response to this surreply.

I would like to just start with the basic premise here and Local Criminal Rule 16 which specifically sets the standard at

open and early discovery. As I indicated, I thought we had reached an agreement on the code.

The government's objections at this point are a little hard for me to grasp because the code itself, is not a classified document. They are not claiming there's any classified information in there. They are not making a national security claim. There's no confidential informant information. There's been no claim that disclosing the code would place agents at risk.

In fact, I have seen nothing but just sort of a bold assertion of the law enforcement privilege. But the threshold showing of why there's potential harm, I am still at a loss. They would not have to disclose the code itself in order to explain, in lay person's terms, what the harm would be. That's a separate issue. So I am still a little bit puzzled by the government's position.

Let me just address briefly the surreply. I understand really there's two points that are made there. One is that they've offered to give us something called the data stream, which is basically a copy, more or less, of information we've already received that shows Pewter's alleged activities and the data associated with that.

When that offer was made, I consulted with both our experts, and frankly their position was this is a red herring; this has nothing to do with the code components that we are

talking about.

For example, the data stream, which is a copy of the data they've said we've received already is, just to give one example based on this identifier information that is attached to it, Mr. Tsyrklevich, on page 3 of his declaration, explained how this identifier information is frequently inaccurate and readily corrupted, and therefore giving us the data stream doesn't address our chain of custody or trial defense issues whatsoever. And I explained that to the government.

I would also note that Agent Aflin is not a code expert. He's somebody who was involved in the investigation. And I have not heard or seen anything from the government that directly challenges either Dr. Soghoian's testimony about what the NIT can do to security settings, or Mr. Tsyrklevich's declaration. I certainly thought that if they were going to file a surreply, that we'd see some contesting of maybe our expert's qualifications or assertions or his security clearance.

They seem to have no objection to our expert, and they have not challenged our expert's statements directly. This data stream issue is indeed a red herring.

I would note, Your Honor, also that we've cited *Budziak*, the Ninth Circuit authority, that even if those assurances were taken at face value, we are clearly not required to rely

on them. This is a case that depends almost entirely on data, tracking of data, possession of data.

As the Ninth Circuit said in *Budziak*, we cited this in our reply at page 6, access to the software, in this case code, is crucial to a defendant's ability to assess the program and the testimony of agents who build the case against them is obviously relevant and material to the defense.

The other surreply point, as I understand it, and really this would be solely if it didn't need to be addressed, but what their point is, that the images that are alleged, in Mr. Michaud's defense, were ultimately found on thumb drives.

Well, thumb drives don't connect to the Internet, and images don't drop on to thumb drives out of the air. The only way data or images get on thumb drives is that if those thumb drives were connected to a computer.

So any of the security overrides or virus issues that are clearly going to be essential to our defense pertain to the thumb drives just as much as the hard drive. They are just simply a different area on the computer that is removable to store information.

With all due respect, that is simply not a relevant response to this case. Again, in *Budziak*, the Ninth Circuit emphasized that the Court itself should not defer to the government's assurances. Obviously we need to do this independently.

So let me get back to what I am trying to understand is the government's problems here. We agreed to the security procedures that they requested. We have one expert whose qualifications and discretion they have not challenged, who is willing to view this stuff at a government facility. So they don't even have to hand him a copy of this stuff.

They proposed a protective order which the Court signed off on, that is in place and we do not object to. And so I am puzzled where the security risk is. Apart from the fact they haven't shown a harm by disclosing the code to us, there has been no discussion or no recitation to the fact that the measures they requested we've agreed to, and even if there were potential harm, are adequately addressed by what the Court has already issued in the code protective order; it is an independent order.

So Your Honor, really what it comes down to is this idea of relevance. The government itself in its pleading says evidence is material under Rule 16 if it is helpful to a possible defense.

In fact, the Ninth Circuit's standard is substantially broader than that. It is helpful even if they've allowed us to investigate and focus or eliminate potential defenses. But the government recognizes, I think, that this is relevant. And then the real issue: Are these security precautions adequate?

If the government wants additional precautions, we have invited them to suggest those. We are not looking to circulate this stuff. We just need to look at it.

Finally, Your Honor, I would point out that I am concerned -- a little bit of a preview we got during the hearing about what I saw as a sword and shield element. We went forward at the hearing based upon a very -- just partial code information we got, primarily based on the government's assurances that the material we've gotten was sufficient and relevant for that hearing.

Then Dr. Soghoian is following up on Agent Alfin's testimony about how NITs works, and we get the objection, well he didn't look at the code.

It puts us in a very difficult position. I respectfully submit this is going to get much worse at trial because basically everything that they are putting in is related to this computer and its security provisions and their ability to indicate who was on the computer or who downloaded on this computer, whose activities were on the computer.

So, Your Honor, I think this is actually fairly straightforward because we have agreed to all their security provisions. It is obviously relevant evidence. And unless the Court has any specific additional questions about how we would handle this or other concerns, I would stand again on the rest of our pleadings.

THE COURT: Okay. Mr. Hampton.

MR. HAMPTON: Good morning, Your Honor. I think it is important in understanding this motion that the defense maintains that the evidence they seek -- the information they seek is obviously relevant. That's certainly -- if that were true, we might have a different case, but I don't think it's obviously relevant.

If we look at the pleadings we see that, from the defense prospective, that identify four questions, and I think they say this information is necessary.

So first the defense would say, well, how do we know the unique identifier was unique? We have to see who generated it, because we don't know if it is unique. If we don't know it's unique, then we don't know if the information that we believe is associated with Mr. Michaud, we don't know if that is accurate.

Well, Your Honor, the government checked the database. The identifier assigned to Pewter as a result of the NIT was unique. The identifiers for all the targets of the investigation were unique.

The defense also says, well, we need to know if the NIT data were accurate. The government has provided the data that we obtained as a result of the NIT, the IP address, the MAC address, the other information that was stored in our database and that we've received.

The government has provided the code, as it agreed to provide, the code that generated that data, so that the defense and its expert can evaluate whether in fact that code could have generated the data that we have.

And the government has offered to provide to the defense the network stream, the packet information that was transferred from Mr. Michaud's computer when the NIT was active, to the government controlled servers, which recorded that data.

So if what Mr. Michaud and what the defense wishes to do is to verify, as they say in their reply, that the information that the government obtained as a result of the NIT and that resulted in its identification of Mr. Michaud were in fact accurate, the defense has the tools that they need to do that.

The third question that the defense asks is, well, what if the government sent something else, the government sent some other program and it seized some other information or conducted some other searches on Mr. Michaud's computer? Well, first of all, we didn't; the government didn't. The government sent the NIT. The NIT obtained, I believe, six or seven unique pieces of information pursuant to a warrant. It sent that information back to the government. And that is the information the government has disclosed to the defense.

But even if there is some other data that were seized, the government isn't relying on that. We haven't proffered any

evidence based on that. If we did, certainly the Court could and should take appropriate action; that would not be proper for the government to sandbag the defense in that way. We are saying we don't have other information. That is true and accurate based on what we know at this time. And I don't see any justification for second-guessing that.

The fourth question, and it is related really to the third question: Well, what if someone else is responsible for the child pornography on Mr. Michaud's devices? What if someone else, whether the government or some other entity, put a virus on his computer or allowed that child pornography to get there? Well, again, the government didn't do that. And if someone else did, it would seem that the defense ought to be able to come up with some justification for that theory in the devices that are available to them, the data, the forensic images of those devices, the forensic image of Mr. Michaud's computer.

So far as I understand it, they haven't yet done their full forensic investigation of that evidence. So the defense isn't saying, well, I've looked and I can't tell and here's why. They just haven't done that yet. They rather, in fact, look at the information that they say we have.

Now, the defense has also, I think in some ways, turned this inquiry on its head. They seem to be taking the position that they are entitled to this information, we haven't shown

why we shouldn't give it over. But that is actually not how discovery generally works. The defense has to demonstrate some entitlement to the information, which we maintain they haven't done.

Now, in this instance, if the Court were persuaded that the defense has made some showing, the government does have grave concerns about disclosing the information that is requested. And I will get to that at the end. But we do believe there would be harm and we will articulate that.

But as to this notion of materiality, I simply don't believe that the defense has made a showing, nor does the *Budziak* case change things.

In that case, the software program and software code that was at issue was absolutely central to the issues at trial. The defendant had stipulated to all the other elements of the offense -- the offense was possession of child pornography -- and I believe all the other elements of distribution, except for the distribution itself.

So that law enforcement software program, where the undercover downloaded child pornography from the defendant in that case, it was critical. It was critical to the government's proof. It was critical to the case. And so the Ninth Circuit held that the government had to disclose more information about that program, and that the district courts could not simply rely on the government's assurance it didn't

matter.

Here, we have a very different case. The information obtained by NIT does not go to the core of this case. It is not required to prove the essential elements of the offenses, possession of child pornography and receipt of child pornography.

It is relevant. I don't mean to say that it is not. It is certainly true that if there were some inaccuracy in the IP address, that could present a problem. The IP address was how the government identified the defendant. It is how it obtained the search warrant in this case. But in terms of a trial, that information, the IP address, the MAC address, it certainly explains why the government did what it did. And it would no doubt be part of the narrative, or could be part of the narrative in the government's case, but it is not required to prove the essential elements of the charges, certainly not as to the possession.

So I don't think that the Ninth Circuit's opinion has a lot of bearing on this case and how the Court should resolve this particular dispute.

And that brings me to the final matter, which is the matter of the law enforcement privilege. And the government, as the Court -- sorry, the government is aware and has, both in the defense's reply and the remarks of the Court, it understands the concern about the notion of an ex parte

in-camera hearing, and it understands why there is discomfort with that.

It also understands that to this point the government's articulation of the harm, the reason it is so deeply concerned about further disclosure related to the use and deployment of the NIT has been, I think, at best, circumspect. And unfortunately that is in part due to the nature of the information and what the government is worried about disclosing.

What the government is prepared to do at this time is, to the extent the Court believes it would be necessary to consider these issues, consider the law enforcement privilege. The government does have an affidavit from a special agent with the FBI and the government would propose filing that under seal, if the Court will take it under seal. The government will also, rather than provide it ex parte, would be willing to provide a copy to the defense subject to the existing NIT protective order, and that is how we would propose to proceed.

We would simply ask, after the Court reviews the affidavit, if it concludes that it does not wish to file it under seal, then the government would wish to withdraw that affidavit. It does not want it in the public record. But given that it would be produced subject to the protective order, it has no problem with the defense keeping a copy.

So Your Honor, if I may approach.

THE COURT: Wait a minute, I want to hear on that.

MR. FIEMAN: Your Honor, obviously we can proceed this way, we have no objection. Really our objection is why didn't we do this last week so I could come in and make an informed presentation, talk to my experts. You know, we have been harping on this from the beginning --

THE COURT: We are doing it now.

MR. FIEMAN: Yes, thank you, Judge.

THE COURT: It may be filed under seal and remain under seal and under the protective order that is in place.

MR. HAMPTON: Your Honor, may I approach?

Your Honor the defense's point is well taken. This is not an effort on the part of the government to delay unnecessarily, but as I would hope the Court and the defense will understand, these issues are important. They have high stakes. And the government has been working hard speaking with -- it is not simply Mr. Becker and myself who have to make these decisions, but our management, and more importantly management within the FBI and the law enforcement agencies who care deeply about these issues. So we are doing our best.

MR. FIEMAN: Your Honor, I withdraw any objection to the submission of this affidavit.

THE COURT: I am sorry --

MR. FIEMAN: I withdraw any objection to the

submission of this affidavit.

THE COURT: All right. Well, let me read it.

(Pause.)

THE COURT: Okay.

MR. HAMPTON: Unless the Court has any further questions, I don't have anything further to add.

THE COURT: Mr. Fieman.

MR. FIEMAN: Thank you, Your Honor. I withdrew my objection because I don't see anything here that adds to what we already know.

The discussion here is about disclosure to the public or in open court. We are not asking for that at this point. We are asking to follow the government's protective order, which is extraordinarily restrictive. I mean, we are sending one expert to an FBI office to look at the code.

I do not see any challenge here to our expert's assessment of the relevance. It seems to be largely a restatement of the government's existing position.

And Your Honor, I would note we appreciate the government's assurances. It is not an issue about their personal integrity. But so often, when the defense has found issues, particularly in these data-driven cases that have extraordinary impact, I would refer the Court to our case, the Robert Lee case in front of Judge Leighton, there was tremendous resistance to turning over the software there. We

ended up going with a virus infection defense that resulted in acquittal of five out of the six charges. So we have some experience with materiality.

I would note, Your Honor, we can't reverse engineer this. We have consulted with all of our experts. The one thing particularly that's not discussed here is the security overrides. We know from Dr. Soghoian's testimony that basically the fences were down from this malware, and we cannot reverse engineer it until we know exactly what security provisions were overriden, including what thumb drives may have been infected.

So, Your Honor, starting with the presumption that discovery is appropriate, is relevant, we ask the Court to just pursue the protective order that is already in place.

Our only additional request, if you are inclined to rule in our favor, Your Honor, is that we do believe this has been dragged out since -- really since September when we made the initial request, and we ask this be done expeditiously.

THE COURT: Well, first I am satisfied that the defense has shown materiality here to preparing the defense. I don't need to discuss that in depth, in my view. I think the papers speak for themselves. And it may be a blind alley, but we won't know until the defense can look at the details of what was done.

So far as the privilege is concerned, what has been

presented is nothing more than a showing that disclosure could possibly lead to harmful consequences. I think that is not sufficient to justify a separate hearing as originally was requested, and I think the affidavit filed basically says the same thing that the government said in their brief on page 13, that disclosure could possibly lead to a variety of harmful consequences.

It is my opinion that the protective order in place is sufficient to protect this information, and it is my judgment that the motion should be granted. The material requested should be submitted, but under the terms of the protective order in place.

If there are other additions or changes that need to be made to the protective order, you can discuss that and submit those things to me. That is my ruling on this matter.

Now, you know, behind that ruling is this: The government hacked into a whole lot of computers on the strength of a very questionable search warrant. I ruled on the admissibility of that in what I considered to be a very narrow ruling.

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. And the government should respond under seal and under the protective order, but the government should respond

and say here's how we did it.

So, you know, I guess what I am saying is that this whole thing didn't seem that complex to me. I respect the government's position in trying to keep this under wraps. I think it can be done by the protective order adequately.

So the defendant's third motion to compel discovery is granted. Do you have something else, Mr. Hampton?

MR. HAMPTON: Your Honor, could we have just a moment? We may have a question.

(Pause.)

MR. HAMPTON: Your Honor, in light of the Court's ruling, both Mr. Becker and I will need to consult with our supervision. We will also need to consult with the FBI, as I think there may be real reluctance to be able to produce any of this material.

So I wonder if the Court could set a timeframe, perhaps in two weeks, so we can report to the Court whether or not we can comply with the Court's order.

THE COURT: It seems to me you can either produce it or move to dismiss. You are going to have the same problem in the other 130 cases, whatever you have, based on the same information.

But I think that is a reasonable request, in light of the long delay in trial that I guess we have all agreed to, a couple of weeks.

MR. FIEMAN: I strongly object, Your Honor. Without involving the Court in the government's settlement proposals and everything, again, frankly from our perspective, this is a delaying tactic to try and force Mr. Michaud to make a choice on the five-year mandatory minimum on the receipt or try and take some other option. They set deadlines on that. And frankly they are trying to run out the clock on some of our options.

I would ask the Court to just let its order stand. We'll work out the timing. If we can't work out the timing, then we would revisit.

THE COURT: I am not involved in your settlement negotiations. But it seems to me that those things should also be -- any artificial deadlines set by the government should also be set over.

MR. FIEMAN: Thank you, Your Honor.

THE COURT: But they don't have to do what I suggest to them in that regard.

There's also, of course, always a possibility of an interim appeal or whatever. But you know, do whatever you think is right.

MR. HAMPTON: Well, Your Honor, then I guess the parties will -- the Court's order will be entered today and the parties will proceed accordingly.

THE COURT: I am sorry, I didn't hear that.

MR. HAMPTON: Since the Court's order will be entered today and the parties will proceed accordingly, we will consult with our supervision and the FBI and make a decision as quickly as we are able.

THE COURT: Yes. Well, you know, it is of questionable propriety for me to get into settlement negotiations, but it would be a damn dirty trick if the government is using these discovery issues as a weapon to force a decision on a plea agreement before things are resolved. So you can do what you want, I guess.

The motion is granted and we'll go from there.

MR. FIEMAN: Thank you, Your Honor.

MS. SULLIVAN: Thank you, Your Honor.

THE COURT: Ordinarily, the clerk will enter a minute order that I have granted the motion subject to the protective order. That is all the order that you need.

MR. FIEMAN: Thank you, Your Honor.

MR. HAMPTON: Thank you, Your Honor.

(Proceedings concluded.)

* * * * *

C E R T I F I C A T E

I certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

/S/ Teri Hendrix _____ February 17, 2016
Teri Hendrix, Court Reporter Date

JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, Defendant.	No. CR15-5351RJB DECLARATION OF COLIN FIEMAN

I, Colin Fieman, declare under penalty of perjury that the foregoing is true and correct:

A. The Discovery Timeline.

1. The defense first requested production of the discovery that has now been ordered by the Court on September 9, 2015. The Government refused the request and the defense filed its First Motion to Compel Discovery on November 20, 2015 (Dkt. 54).

2. On December 4, 2015, the Government filed a brief in opposition of discovery. (Dkt. 74). In that brief, the Government argued (as it does in its Motion for Reconsideration) that the code was subject to a "law enforcement privilege" and that its disclosure would be "harmful to the public interest." *Id.* at 15.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Exhibit B-001

3. On December 10, 2015, the Government notified the defense that it was withdrawing its objections and agreed to disclose the NIT discovery. This agreement was noted on the record on the December 14, 2015, discovery motion hearing. *See* Dkt. 115-2 (December 14 hearing transcript) at 2-3. At that time, the Government stated that it would seek to complete discovery by "the first week of January." *Id*. at 36.

4. 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 Government had requested for ensuring that the NIT data remained secure and confidential. The Court issued its NIT data protective order the same day (Dkt. 102).

5. On January 11, 2016, the Government provided a disc to the defense that contained only a portion of the relevant discovery. On January 14, 2016, the defense filed its Third Motion to Compel Discovery (Dkt. 115). The Court ultimately scheduled a hearing on the motion for February 17, 2016, and in the interim the Government filed the following pleadings and declarations: **Dkt. 123** (Govt. Response to Request for Expedited Discovery Hearing); **Dkt. 134** (Govt. Response to Third Motion to Compel Discovery); **Dkt. 156** (Govt. Surreply to Third Motion to Compel); **Dkt. 157** (Declaration of Special Agent Daniel Alfin).

6. At the hearing itself, the Government elected not to call any witnesses, but submitted another declaration under seal from Special Agent Robert Stone (**Dkt. 160**). The Court, after reviewing this additional declaration, found it "basically says the same the thing the government said in their brief on page 13." Exh. A (February 17, 2016, hearing transcript) at 18.

7. The Government elected not to pursue an interlocutory appeal of the Court's ruling on February 17. Instead, the Government asked the defense to agree to a

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

March 28 deadline for responding to the order so that it could have additional time to consult with various agencies and "stakeholders."

8. The defense agreed to the extension, and also notified the Government that it was amenable to submitting a proposed revised protective order if there were additional security conditions that it concluded were necessary. Although the Court had found that the code discovery protective order that had previously been submitted by the Government was sufficient (*see* exh A. at 18), it has never been the defense's intention to force the Government to reveal sensitive information in open court or otherwise undermine legitimate security interests. The response from the Government came in the form of its Motion for Reconsideration, filed on what had been the agreed deadline for production.

B. The Objections and Arguments in the Motion for Reconsideration Have Been Previously Raised, Addressed and Resolved by the Court.

1. The Government's Claim that the Discovery is Not Material.

9. The Government's Motion for Reconsideration does not contain any facts, arguments or citations that were not already included (sometimes several times over) in its prior pleadings. Moreover, the Government acknowledges that the ex parte pleading it is seeking to submit does not contain any new facts or arguments bearing on the Court's finding that the discovery is relevant and helpful to the defense. Instead, it would only pertain to the purported harms that might ensue if the FBI complies with the Court's order. Motion for Reconsideration at 3-4.

10. Pursuant to L. Cr. R. 12(10)(A), a Motion for Reconsideration should be denied "in the absence of a showing of manifest error in the prior ruling or a showing of new facts or legal authority" that could not have previously been brought to Court's attention with "reasonable diligence." Since the Court is already familiar with all the facts and pleadings, this declaration will simply cross-reference the main points in the

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Exhibit B-003

Motion for Reconsideration with the places where the Government previously made the same points.

11. Most broadly, the Government previously argued in both its Response to Defendant's Motion to Compel and its Surreply to Motion to Compel that the discovery is "not material to [the] defense" and "irrelevant to any purported suppression issues or defense at trial." *See, e.g.*, Dkt. 134 at 2. Likewise, the Government maintains in its Motion for Reconsideration that the defense "has made no showing that would support the requested discovery" and persists in characterizing the defense's showings of relevance as "speculation." Dkt. 165 at 8, 10; *compare also, inter alia*, Dkt. 156 (Govt. Surreply) at 3 *and* Motion for Reconsideration at 8 (repeating, almost verbatim, its arguments about the relationship between thumb drives and data originally stored on a computer).

12. As previously briefed, evidence is 'material' under Rule 16 if it is helpful to the development of possible defenses. *United States v. Olano*, 62 F.3d 1180, 1203 (9th Cir. 1995). Information is also material "even if it simply causes a defendant to 'completely abandon' a planned defense and 'take an entirely different path.'" *United States v. Hernandez-Meza*, 720 F.3d 760, 768 (9th Cir. 2013) (quotation omitted). The Government has not disputed this legal standard, nor does it do so now.

13. Although a defendant is not required to explain his or her trial strategy to establish materiality, Mr. Michaud has made a substantial proffer about some of the pre-trial issues that are implicated by the discovery and also indicated how it was important to potential defenses. *See* Dkt 149 at 4- 8. Based on these proffers and all of the previous pleadings, the Court had no trouble concluding that it is "satisfied that the defense has shown materiality here to preparing the defense." Exh. A at 17.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

2. The Government Repeats its Disagreements with Defense Experts.

14. In its Motion for Reconsideration, the Government goes on to assert that "[e]ven Michaud's own expert declaration does not support his claimed need" (referring to Vlad Tsyrklevitch's declaration, dkt. 115-1). Motion for Reconsideration at 9. The declaration speaks for itself (succinctly and effectively) in refuting that odd contention, and the Court apparently agrees, since it noted at the February 17 hearing that the defense had not only shown materiality, but "the papers speak for themselves." Exh. A at 17.

15. Moreover, the Government levelled the exact same challenges to the defense's experts prior to the Court's ruling. *See, inter alia*, Dkt. 134 (Response to Defendant's Motion to Compel) at 7 (arguing that the defense "has everything he would need to 'independently determine'" the issues he has raised and "nothing in Michaud's motion or the declaration from his expert says otherwise."); *compare also* Dkt. 166-2 at ¶¶ 4-7 (second declaration of FBI Agent Alfin, who repeats most of the Government's disagreements with the defense's experts and states his opinion about whether the NIT discovery is relevant to the defense).

16. The Government also ignores (as it did in its prior pleadings) the unrebutted testimony of Dr. Chris Soghoian. *See* Dkt. 149 (Reply to Govt. Response to Motion to Compel) at 7; *see also* exh. A (February hearing transcript) at 5 (summarizing other deficiencies in the Government's responses to the defense's experts).

3. The Government's Claims That the Discovery is Not Needed to Verify the Accuracy of its Data and Evidence or "Confirm that the Agents did not Exceed the Scope" of the NIT Warrant (Motion for Reconsideration at 6-8).

17. The Government made these arguments in both its Response and Surreply. *See* Dkt. 134 at 11-12; Dkt. 156 at 1-2. The defense cited the relevant facts

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

and authority for disclosure in both its initial discovery motion (Dkt.115 at 4) and in its discovery reply briefing (Dkt. 149 at 6-9).

18. In particular, the Government repeats its assertion that a copy of a "data stream" is an adequate substitute for the discovery sought by the defense. *Compare* Motion for Reconsideration Motion at 6, *with* Govt. Surreply (Dkt. 156) at 1-2 and First Declaration of Agent Alfin (Dkt. 157) at ¶¶ 6-8.

19. The "data stream" issue was previously addressed in both Vlad Tsyrklevitch's declaration and at the February 17 hearing. *See* exh. A (transcript) at 4-5 (explaining – without rebuttal from the Government -- that access to the "data stream" is a "red herring" because it relies on the accuracy of "identifiers"); Dkt. 115-1 at ¶ 6 (identifier errors, on which the validity of a data stream depends, "are pervasive in modern software").

20. Indeed, the Government now concedes that there is at last a "theoretical" possibility of a problem with unique identifiers, but urges the Court to vacate its discovery order because Agent Alfin is personally satisfied that there was no problem with the identifiers in this case. *See* Motion for Reconsideration at 7, lines 18-21; Dkt. 166-2 at ¶ 11. The Government offered the same self-serving statement in the first declaration submitted by Agent Alfin. *See* Dkt. 157 at ¶ 7.

21. Moreover, all of this back and forth on the part of the Government ignores its core obligation to disclose all information relevant to data verification and "chain of custody" issues, regardless of its view of how accurately preserved its evidence may be. *See* Dkt 115 (Third Motion to Compel Discovery) at 4 (citing the relevant case law).

22. Significantly, the Government also continues to ignore (as it did in its prior pleadings) the leading case on discovery of computer data, *United States v. Budziak*, 697 F.3d 1105, 1112-13 (9th Cir. 2012) (holding that "the district court should not merely defer to government assertions that discovery would be fruitless.").

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

DONE this 22nd day of April, 2016.

s/ Colin Fieman
Colin Fieman
Assistant Federal Public Defender

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Exhibit B-007

To: All Tech Agents, Tech Advisors, and Tech Supervisors

From: SSA [redacted], Program Manager, Special Projects Program

Subj: Special Project Concealments

Over the past week, I have received two ECs form the field which describe in GREAT detail surreptitious entries and special project concealments installed in the target locations. These ECs describe the equipment concealed, item in which the equipment was concealed, and where the concealments were placed. These ECs were drafted by case agents, uploaded in ACS, and placed in the case file.

TTAs should not be providing such detail to case agents. One reason TTAs do not testify is to protect our trade craft. If the case agents have this information, they will be required to reveal it during cross examination at trial. Also, an AUSA my require the EC be turned over during discovery before trial. We need to protect how our equipment is concealed and where our is concealed.

It is sufficient for the case agent to simple state that, pursuant to a court order, equipment was installed in the target location.

Exhibit C-001

From: [redacted]
To: MP All Agents
Date: Thu, Apr 17, 2003 10:18 AM
Subject: Revealing techniques

b6
b7C

Over the past few months, ERF has expressed concern about Tech Agents revealing technical details to Case Agents and especially to AUSAs. There have been several instances of AUSAs becoming familiar with our techniques, then resigning and becoming defense lawyers. There also is concern about retiring Agents performing investigative work for defense counsel (i.e. right here in MP).

Attached is a wpd regarding the problems with revealing techniques to active Agents.

In the future, the tech guys may be a little mum about how we're doing things. Just tell us what you need, and we'll do our best to accommodate you. If an AUSA desires to be briefed on a technical issue, we'll try to get it cleared through both ERF and MP management.

Thanks,

[redacted]

Exhibit C-002