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, [redacted] 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. [redacted] The Government further acknowledges that "there may be consequences for this refusal." [redacted] 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) [redacted] 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 [redacted]. To the contrary, the Government briefed its prior motion for secret proceedings at some length. *See* [redacted]

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

[redacted] 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.

[redacted]. 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* [redacted]

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

[redacted]

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. [redacted]

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 [redacted] 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* [redacted]

[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 [redacted] The FBI has staked out this position despite the fact that the discovery sought by the defense [redacted] 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 [redacted]

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

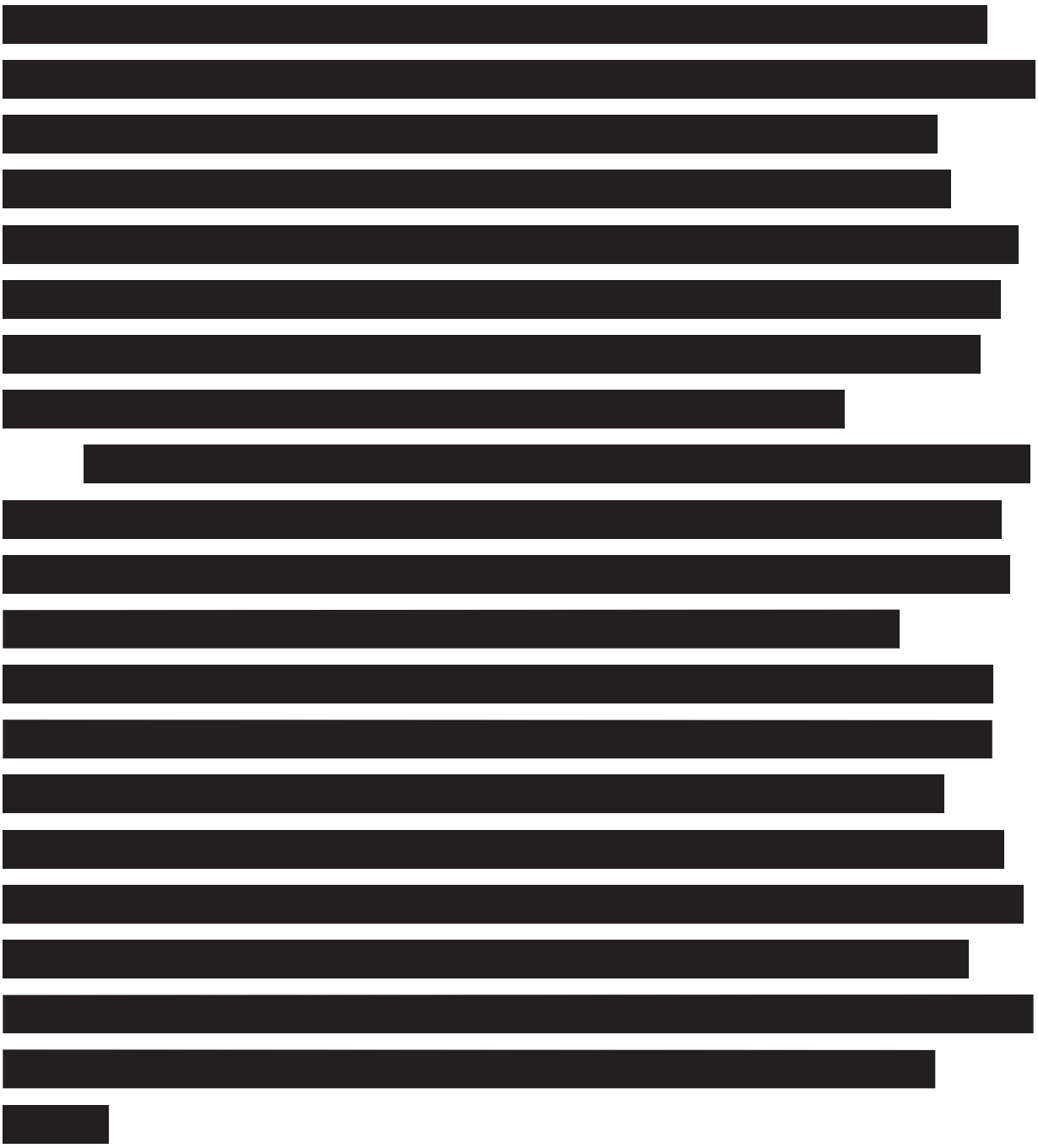
The Government seeks to bolster its Motion for Reconsideration with renewed requests for ex parte and in camera proceedings. [redacted]

Moreover, despite the numerous pleadings and declarations that the Government filed prior to the Court's discovery order, [redacted] 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

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

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



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).

[redacted] *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.").

[redacted]

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). [redacted]

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. [redacted]

In sum, [redacted]

And, finally, the Government has made no showing as to why sealing its proposed pleading or submitting it under a protective order [redacted] 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, [redacted]

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" [redacted] 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; [redacted] and it has flatly refused to adopt additional security measures for discovery that would address any legitimate security concerns.

[redacted] *See also Roviaro*, 353 U.S. at 60 (When a trial court has found that discovery "is relevant and helpful to the

[redacted]

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").

[redacted]. 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 [redacted] 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. [redacted] 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. [redacted] 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 [redacted]

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