JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. DAVID TIPPENS, Defendant.	No. CR16-5110RJB **REPLY MEMORANDUM IN SUPPORT OF MOTION TO EXCLUDE EVIDENCE** *[Oral Argument Requested]*
UNITED STATES OF AMERICA, Plaintiff, v. GERALD LESAN, Defendant.	No. CR15-387RJB **REPLY MEMORANDUM IN SUPPORT OF MOTION TO EXCLUDE EVIDENCE** *[Oral Argument Requested]*
UNITED STATES OF AMERICA, Plaintiff, v. BRUCE LORENTE, Defendant.	No. CR15-274RJB **REPLY MEMORANDUM IN SUPPORT OF MOTION TO EXCLUDE EVIDENCE** *[Oral Argument Requested]*

I. REPLY ARGUMENT

A. The Applicable Law

The Government maintains that discovery is material and subject to disclosure under Rule 16 "only if it is helpful to the development of a possible defense." Govt. Response at 4. As set forth in the defendants' motion to exclude, the NIT code discovery is helpful to several possible defenses. *See* dkt. 31.[1] Moreover, the Government misstates the law, because defendants are entitled to much broader discovery to ensure their constitutional rights to effective representation and a fair trial. *See* dkt. 31-1 (Transcript of *Michaud* Findings and Order) at 21 (Finding that "the discovery withheld implicates the defendant's constitutional rights").

In *United States v. Soto-Zuniga*, __ F. 3d __, 2016 WL 4932319 *8 (9th Cir. Sept. 16, 2016), the Ninth Circuit reaffirmed that "[m]ateriality is a low threshold." The Government is required to disclose evidence even if it does nothing more than assist in the in development of pre-trial motions or may lead to admissible evidence. *Id.*

In fact, the Government is required to disclose evidence that may be *inconsistent* with potential defenses. Evidence is "material" for discovery purposes "even if it simply causes a defendant to completely abandon a planned defense and take an entirely different path." *Id.*, citing *United States v. Hernandez-Meza*, 720 F.3d 760 (9th Cir. 2013).

In *Soto-Zuniga*, the defendant had been arrested for drug trafficking after the police searched his car at an immigration check point. *Id.* at *2. For the purpose of developing potential motions, the defense sought disclosure of stop and arrest statistics for the check point, which were relevant to whether it was constitutional. *Id.* at *5. The defendant also sought law enforcement records related to third parties who may have

[1] Docket citations refer to the docket entries in *Tippens*.

been responsible for placing drugs in his vehicle, although there was no direct evidence that they were. *Id*. at *8.

Much like the arguments the Government has made here, it argued in *Soto-Zuniga* that the defense had made no showing of materiality; had offered no evidence that agents had acted unlawfully; and had failed to show that a third party might be responsible for the alleged crimes. *See id*. The Government also argued that Soto-Zuniga's discovery demands amounted to "a fishing expedition," a claim it makes about the discovery requests in this case. *See Soto-Zuniga*, 13-CR-02706-AJB (S.D. Cal.), Dkt. 23-1, November 24, 2013; Govt. Response to Motion to Exclude (dkt. 58) (Govt. Response) at 4.

The district court denied the defendant's discovery demands, finding that they were unlikely to lead to admissible evidence and that granting the requests would needlessly prolong the case. 2016 WL 4932319 at *7. The trial court also observed that "I don't think putting the Government through the effort of now having to go back and come up with an analysis to satisfy your curiosity would be appropriate," and that "I don't see there is any smoke to which we could suggest there would be fire in this case." *United States v. Soto-Zuniga*, Ninth Circuit No. 14-50529, June 8, 2015, Excerpts of Record (dkt. 10) at 153. In essence, the court denied discovery on the same basis that the Government puts forth here—that the defendant has not made a strong enough showing that providing the documents would prove fruitful.

On appeal, the Ninth Circuit held that not only was the defendant entitled to the discovery, but that the trial court had abused its discretion by not ordering it. Importantly for purposes of this case, the court also held that the "sensitive nature" of some of the law enforcement records at issue was immaterial. 2016 WL 4932319 at *8.

Recognizing that the Government might have legitimate reasons for not wanting to disclose the records, the Ninth Court nevertheless ordered the trial court to grant the defendant's discovery motion. The only concession to the Government was that the trial court was also instructed to "consider the government's request for a window of time before production to determine whether to continue to pursue this case, and to consider the government's request for protective measures that would maintain the security of the information in the documents while allowing Soto-Zuniga to adequately prepare a defense." *Id*.

In this case, the defense has offered every possible accommodation to the Government in terms of protective measures. And no matter how sensitive the NIT discovery may be, that has no bearing on the fact that, as this Court has concluded, it is "central to the case, it's central to the search warrant that was issued, it's central to the proof that might be offered at trial, it is the background for the whole case." Dkt. 31-1 (transcript of *Michaud* findings and order) at 19. Under these circumstances, the Government should be given a window of time to choose between production and sanctions.

Finally, while ignoring *Soto-Zuniga* (as well as *Hernandez-Meza*, *Budziak*, and all of the other cases cited in the defendants' motion), the Government misconstrues *United States v. Armstrong*, 517 U.S. 546 (1996). *See* Govt. Response at 4. The Ninth Circuit has explained the limited application of *Armstrong*: "Notwithstanding that language and guidance of the Supreme Court, we do not read *Armstrong* to preclude Rule 16(a)(1)(E) discovery related to the constitutionality of a search or seizure. In our view, the holding of *Armstrong* applies to the narrow issue of discovery in selective-prosecution cases." *Soto-Zuniga*, 2016 WL 4932319 *6 (Sept. 19, 2016) (citations omitted); *see also United States v. Thorpe*, 471 F.3d 652, 657 (6th Cir. 2006) (discussing *Armstrong* and noting that, even when discovery is related to a selective-prosecution claim, all a defendant need do is produce "some evidence" of discrimination to obtain the discovery).

The Government's reliance on *United States v. Matish* and *United States v. Darby* is also misplaced. Govt. Response at 11. Both these cases were decided in the Eastern District of Virginia, where the NIT warrant was issued, and not in the Ninth Circuit. The *Matish* decision is an outlier in its reasoning in several ways, most notably for holding that people do not have a reasonable expectation of privacy in their computers. 2016 WL 3545776 at *22-23. And, as the Government's quotation from *Darby* demonstrates, the judge there was satisfied with Agent Alfin's declarations about why the defense did not need discovery. *See* Govt. Response at 11.

B. The Levine Declaration

The decision in *Soto-Zuniga* confirms the soundness of this Court's exclusion order in *Michaud* and makes plain that the Government must elect between production and inviting discovery sanctions in the instant cases. While the Government has supplemented its discovery pleadings with a declaration from Prof. Brian Levine, this declaration does not change the discovery equation for several factual and legal reasons.

1. Levine's Lack of Foundation for his Opinions and Lack of Relevant Expertise

Even if Levine's declaration could be taken at face value, all it establishes is disagreement about complex technical issues between the Government's sole expert and the defense's six experts (Tsyrklevitch, Miller, Kasal, Young, Soghoian, and now Prof. Leonid Reyzin of Boston University, *see* exh. D). Prof. Levine has never previously worked on a NIT case and his research in unrelated areas is funded by the FBI. Levine Declaration at ¶ 1. In contrast, both Prof. Matthew Miller and Shawn Kasal in particular have done extensive analytical work in *United States v. Cottom* and the related NIT cases. *See* dkts. 31.3 and 31.5.

Second, Levine has not looked at or analyzed the NIT discovery that he is opining about. Levine Declaration at ¶ 3. Instead, he acknowledges that "I have not had access to nor did I review the source code or executable for the FBI exploit that deployed the NIT payloads. I also have not had access to nor did I review the FBI server or any 'generator' code used to create unique identifiers." *Id.*; *compare* Govt. Response at 8 (asserting that Levine "has looked at the available information, including the network data.").

It is not surprising that the FBI has not allowed Prof. Levine to examine the components, given its practice of withholding the details of its hacking capabilities not only from defendants and judges, but prosecutors and case agents as well. *See* Brad Heath, *FBI Warned Agents Not to Share Tech Secrets with Prosecutors*, USA Today, April 20, 2016 (reporting on FOIA disclosures documenting the FBI's practice of withholding information from prosecutors and agents);[2] *see also* Garrett Graff, *The Law Isn't Keeping up With Technology*, The Washington Post, September 23, 2016 (reporting on DOJ's efforts to limit disclosures in cyber prosecutions and how "[t]his situation is stymieing criminal investigations, upending innocents' lives and making it harder to set legal boundaries around mass-surveillance programs. The result is that, when it comes to technology, justice is increasingly out of reach").[3]

Even if DOJ had shared the NIT exploit and other code with Prof. Levine, it is not clear that he has the training or experience necessary to render reliable opinions. He has not published any papers on malware or software exploits, and his *curriculum vitae* does not list any experience developing or analyzing malware or exploits. As the Government itself has acknowledged elsewhere, "[t]he vast array of digital hardware and software available requires even digital experts to specialize in particular systems and applications." Exh. A at ¶ 38(a) (Excerpt of August 31, 2016, Affidavit of

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

[3] Available at: https://www.washingtonpost.com/posteverything/wp/2016/09/23/government-lawyers-dont-understand-the-internet-thats-a-problem/?utm_term=.a85a76395164

Homeland Security Special Agent Scott Sutehall in *United States v. Thomas Clark*, MJ16-377).

In contrast, for example, Vlad Tsyrklevich has both developed new software exploits and analyzed exploits developed by others, and has specific, hands-on experience developing and analyzing malware used by government agencies which is directly applicable to the issue in these cases.

As a consequence, Levine is forced to rely in large part on statements from Agent Alfin, who also lacks firsthand knowledge about the exploit and has no relevant expertise. For example, in discussing the issue of whether the FBI's malware disabled security settings on target computers, Levine acknowledges that it is at least "theoretically possible" for the "exploit" component of an NIT to do that. Levine Declaration at ¶ 11. But Levine goes on to dismiss the issue by simply quoting Alfin's unsubstantiated statement that "the NIT used here and the exploit used to deliver it did not do so." *Id*.

Agent Alfin, however, has testified in *United States v. Eure* and in other proceedings that he has not seen any of the NIT components either, nor does he have the expertise to analyze them even if he had. *See also, e.g.*, Levine Declaration at ¶ 9 ("We know *from Special Agent Alfin's sworn statement* that the exploit was restricted to allowing the payload to be delivered and executed and did not alters the settings of the computer"); *id*. at ¶ 34 ("*Special Agent Alfin's sworn statement says*" that he reviewed the identifier data and "*Special Agent Alfin's examination of the output*" indicates that there were no errors) (emphasis added)

In this regard, it is also significant that Prof. Levine says nothing about whether the NIT components were tested and audited in accordance with NIST standards. *See* dkt. 31.5 (Kasal Declaration) at ¶ 8-9. There is no evidence that they were and, as a result, many of Levine's conclusions are comparable to assuming that a Breathalyzer result in a DUI case is correct without knowing whether the machine was calibrated or operated in accordance with the manufacturer's instructions. If a blood alcohol reading is inadmissible at a DUI trial unless the defense has an opportunity to review and challenge Breathalyzer records, it makes no sense for the Government to maintain that comparable discovery is not material in a case involving vastly more complex technology. *See also United States v. Budziak*, 697 F.3d 1105, 1113 (9th Cir. 2012) (reversed due to prosecution's failure to disclose "EP2P" program, where "the charge against the defendant is predicated largely on computer software functioning in the manner described by the government, and the government is the only party with access to that software.").

Moreover, the need for testing and auditing records related to the NIT has been recently demonstrated by the disclosure of Yahoo's secret cooperation with the NSA and FBI to access private emails. The program used for that surveillance contained a basic programming flaw that could give third party hackers access to millions of private accounts, a mistake that led to the resignation of Yahoo's Chief Technology Officer. *See* Joseph Menn, *Yahoo Secretly Scanned Customer Emails for U.S. Intelligence Sources*, The New York Times, October 4, 2016.[4] Likewise, security flaws have been found in surveillance software similar to the FBI's NIT that were used by the German government.[5]

2. Basic Gaps and Errors in Levine's Declaration

Given Prof. Levine's third-hand knowledge, it is not surprising that he hedges his bets and qualifies most of his opinions. For example, Levine says that he is not aware of any "peer reviewed, published articles" discussing the storage of illegal

[4] Available at: http://www.nytimes.com/reuters/2016/10/04/business/04reuters-yahoo-nsa-exclusive.html?_r=0

[5] See https://www.ccc.de/en/updates/2011/staatstrojaner

content on private computers by third parties, as described in Shawn Kasal's declaration. Levine Declaration at ¶ 20; *see also* ¶ 6(b) (where Levine states that there is "no evidence to support" the defense's various "hypotheses," a conclusion that further reading reveals to be largely based on Alfin's assertions).

At the same time, however, Levine does not dispute that Vlad Tsyrklevicth, Shawn Kasal and Prof. Matthew Miller in particular are "clearly qualified" as experts, given their experience working on cases where those very things happened as well as on earlier NIT cases. *See* Levine Declaration at ¶ 17.

Instances of third party attacks and remote storage of illicit pornography are in fact well documented. *See, e.g*, 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.");[6] 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.).[7]

What Levine may not realize is that the Government itself has elsewhere acknowledged that the basic forensic problems and issues set forth in the defense declarations are valid. In a recent computer search warrant application, the Government explained that child pornography found on a defendant's computer could be the result of "malware that would allow others to control any seized digital device(s) such as viruses, Trojan horses, and other forms of malicious software." *See* exh. A. at ¶ 9. And Agent Alfin himself has testified about how such malware is often undetectable and

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

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

"written so that there is no code left behind on the computer." *See* exh. B (September 14, 2016, testimony of Agent Alfin in *United States v. Chase*, CR15-15 (W.D. N.C.).[8]

Similarly, FBI Director James Comey, while describing the possibility that Secretary Clinton's private email server was hacked by Russia, observed that sophisticated malware is often designed not to leave traces behind: "With respect to potential computer intrusion by hostile actors, we did not find direct evidence that Secretary Clinton's personal e-mail … was successfully hacked. But, given the nature of the system and of the actors potentially involved, we assess that we would be unlikely to see such direct evidence."[9]

Given these facts, Prof. Levine's opinion that "[t]he place to look for malware that has purportedly infected a computer is the computer itself" is simplistic and misleading. *Id*. at ¶ 15; *see also* exh. D (Reyzin Declaration) at ¶ 10 (disputing Levine's assertion).

Prof. Levine's general opinions about malware and third party control are also contrary to those of Mozilla, the company that produces the Firefox web browser used by Tor. As Mozilla explained in an earlier submission to the Court, "[t]he information contained in the [second] Declaration of Special Agent Alfin suggests that the Government exploited the very type of vulnerability that would allow third parties to obtain total control [of] an unsuspecting user's computer." *Michaud* dkt. 195 (Mozilla Motion to Intervene) at 10. Plainly, unless the defense knows what that exploit is, it is unable to confirm the actual vulnerabilities.

[8] While Alfin was asked about malware that is designed to "steal someone's information," his testimony applies to many types of malware and viruses, and it is consistent with the conclusions of the defense's experts.

[9] *See* https://www.fbi.gov/news/pressrel/press-releases/statement-by-fbi-director-james-b-comey-on-the-investigation-of-secretary-hillary-clinton2019s-use-of-a-personal-e-mail-system

While the Government and Levine make much of the fact that the defense has not examined any of the defendants' hard drives to look for malware, that point has dropped by the wayside. *See, e.g.*, Govt. Response at 12. Robert Young has recently examined a copy of Mr. Tippens's computer hard drive. Consistent with both Mr. Young's earlier explanation about the impossibility of "reverse engineering" the NIT malware, as well as Alfin's and FBI Director Comey's statements about how malware code is often undetectable, Mr. Young has been unable to "reverse engineer" the NIT or determine what additional security vulnerabilities it created. *See also* dkt. 31-4 at ¶¶ 5-9 (Young declaration).

An additional problem, in Mr. Tippens's case at least, is that the agents who seized his laptop did not follow the standard protocol for preserving the data on it. They shut the laptop down instead of just unplugging it. *See Best Practices for Computer Forensics*, at 3;[10] Forensic Magazine, *Before You Pull the Plug*, April 1, 2010 ("There are justifiable reasons to 'pull the plug' on a live computer rather than perform a normal shutdown. Even just sitting there unattended, numerous processes are ongoing which continually perform reads and writes between the CPU, the operating system, RAM, the hard drive, and so on).[11] While agents did copy the laptop's "random access memory" before shutting it down, this did not capture all of the data and shutting down the computer created a substantial risk that some data was altered or lost. *See also* exh. D (Reyzin declaration) at ¶ 10.

Professor Levine makes a number of other basic errors while dismissing concerns about the FBI's failure to ensure the chain of custody of the data collected by the NIT, such as through the use of encryption. Although Levine's declaration includes

[10] Available at: https://www.oas.org/juridico/spanish/cyb_best_pract.pdf. Notably, the Chair of the Scientific Working Group that issued these standards is Mary Horvath, a Senior Digital Forensic Examiner with the FBI.

[11] Available at: http://www.forensicmag.com/article/2010/04/you-pull-plug

four pages of dense, technical information about this topic, most of the information he presents is irrelevant to the arguments we have made:

To begin, Levine acknowledges that data transmitted between the NIT and the FBI's servers could be intercepted and modified at one of multiple routers and servers located along the path between the target computers and the FBI’s server. Levine declaration at ¶ 28. But Levine goes on to state that “in general, routers controlled by ISPs [Internet Service Providers] are protected by a professional information technology staff and it is reasonable to expect that was the case here.” *Id*. at ¶ 28.

This comment suggests that routers on the Internet are secure and cannot be hacked or accessed by third parties. That is not the case. Indeed, just this summer, a party believed to be the Russian government published some of the code that the National Security Agency uses to hack into Internet routers. *See* Ellen Nakashima, *Powerful NSA Hacking Tools Have Been Revealed Online*, The Washington Post, August 16, 2016.[12] The publication of these tools and the NSA’s router exploits also revealed that the routers had been vulnerable to hacking for several years.[13] In addition to the risk that routers are vulnerable to hacking via unintentional flaws, major manufacturers of routers have also hidden “backdoors” in their products through which third parties with knowledge of the backdoors can covertly gain entry.[14]

[12] Available at: https://www.washingtonpost.com/world/national-security/powerful-nsa-hacking-tools-have-been-revealed-online/2016/08/16/bce4f974-63c7-11e6-96c0-37533479f3f5_story.html.

[13] *See* http://arstechnica.com/security/2016/08/cisco-confirms-nsa-linked-zeroday-targeted-its-firewalls-for-years/

[14] *See* http://arstechnica.com/security/2015/12/unauthorized-code-in-juniper-firewalls-decrypts-encrypted-vpn-traffic/ (describing backdoors placed in routers made by Juniper); https://intelligence.house.gov/sites/intelligence.house.gov/files/documents/huawei-zte%20investigative%20report%20(final).pdf) (House intelligence committee report on the national security threat posed by the use of routers and other telecommunications technology made by Chinese router manufacturers with links to the Chinese military).

It also makes little sense for Prof. Levine to suggest that Tor is "tamperproof." Levine Declaration at ¶ 8. The Tor network is particularly vulnerable to "malicious nodes," which involve users who join the Tor network for the purpose of capturing or corrupting information that is relayed on it. "Just like at coffee shops with open Wi-Fi spots, attackers can intercept network traffic over the air or by running exit relays and snooping on Tor users." Phillip Wintner, *Securing Web Browsing: Protecting the Tor Network*, The Conversation, May 17, 2016.[15]

One notorious instance of this type of tampering occurred when Carnegie Mellon University, while cooperating with the FBI, "compromised the network in early 2014 by operating relays and tampering with user traffic." *Statement from the Tor Project re. the Court's February 23 Order in U.S. v. Farrell*, February 24, 2016;[16] *see also* Bruce Schneir, *How the NSA Attacks Tor/Firefox Users with QUANTUM and FOXACID*, Schneir on Security, October 7, 2013 (reporting on how the NSA interfered with and redirected traffic on the Tor network).[17]

In addition, while Agent Alfin and the government have repeatedly defended the Government's failure to use encryption to provide a tamper-evident way for the NIT and FBI server to communicate, it is notable that Prof. Levine does not defend this decision. As even Agent Alfin has testified, the lack of encryption during the non-Tor parts of the NIT transmissions made the evidentiary data in this case vulnerable to corruption. *See* Motion to Exclude, dkt. 31-6, exh. F at 92.

[15] Available at: http://theconversation.com/securing-web-browsing-protecting-the-tor-network-56840

[16] Available at: https://blog.torproject.org/blog/statement-tor-project-re-courts-february-23-order-us-v-farrell; see also, e.g., Joseph Cox, Confirmed: Carnegie Mellon University Attacked Tor, Motherboard, February 14, 2016 (available at: http://motherboard.vice.com/read/carnegie-mellon-university-attacked-tor-was-subpoenaed-by-feds).

[17] Available at: https://www.schneier.com/blog/archives/2013/10/how_the_nsa_att.html

Making matters even more problematic, Prof. Levine does not know which routers the NIT data was transmitted through along its path to the FBI's server. The Government has provided no information about which organizations were responsible for those routers; how securely the routers were configured; which manufacturers made them; or what if any security incidents those organizations may have experienced during the FBI's Playpen operation. Levine is therefore only able to state that it is "extremely unlikely" that the NIT data was tampered with or corrupted during transmission. *See* Levine Declaration at ¶ 28(b).

Finally, the instant cases themselves amply demonstrate that the Tor browser is vulnerable to malware and hacking, and not just by the FBI. As Mozilla has explained, it has "reason to believe that the Exploit the Government used is an active vulnerability in its Firefox code base that could be used to compromise users and systems running the browser." *Michaud*, dkt. 195 at 3. It therefore makes little sense for Prof. Levine to assert that Tor is "tamperproof" when these very cases illustrate some of its vulnerabilities.

In the final analysis, all that Prof. Levine's declaration establishes are disagreements between him and the defense experts. There are even significant differences of opinion between Levine and Agent Alfin. And Levine offers all of his opinions without having actually looked at the NIT components. He instead relies in large part on declarations by Alfin, which the Court has previously found wanting.

3. Even if the FBI Expert's Opinions had Better Factual Support, the Defendants Would Still be Entitled to the NIT Discovery

Perhaps most basically, even if Prof. Levine's opinions were better supported, the defense would still be entitled to the NIT code discovery. As the Ninth Circuit stated in *Soto-Zuniga*, discovery "is material even if it simply causes a defendant to completely abandon a planned defense and take an entirely different path." 2016 WL 4932319 *8. Defendants are not required to accept the opinions of prosecution experts about the viability of their defenses simply because, like the Wizard of OZ, the prosecution insists that there is nothing to look at behind the discovery curtain.

This is particularly true given that the Government is establishing a track record of unreliability when it comes to disclosures in cases involving advanced technology. *See* Green Kozi, *Who Watches the Watchers?: Judge Blasts DOJ's Refusal to Explain Stingray Use in Attempted Murder Case*, Ars Technica, August 16, 2016 (reporting on hearings in *United States v. Ellis,* during which Magistrate Judge Donna Ryu criticized prosecutors for failing to disclose information about the scope of "Stingray" searches and how the technology functions);[18] *State v. Andrews,* 2016 WL 1254567 at *11-12 (Md. Ct. Spec. App. March 30, 2016) (finding that the FBI had colluded with local law enforcement to conceal surveillance capabilities from the courts and defendants).

Lastly, the Government's focus on evidence that allegedly proves that the defendants' possessed child pornography is not relevant to the discovery issues. *See, e.g.*, Levine Declaration at ¶ 14. All of that evidence is fruit of the NIT searches, and the defendants have a right to discovery for, at a minimum, potential pre-trial motions, including additional suppression motions.

The Government also overlooks the fact that it did not just charge the defendants with possession, but elected to also charge them with the more serious offense of Receipt of Child Pornography. To prove receipt, the Government must prove beyond a reasonable doubt that the defendants knowingly downloaded specific pictures or videos. The defendants intend to argue to the juries that the pictures and videos introduced into evidence by the Government were originally downloaded to the defendants' computers

[18] Available at: http://arstechnica.com/tech-policy/2016/08/judge-blasts-dojs-refusal-to-explain-stingray-use-in-attempted-murder-case/

as a consequence of the FBI's deployment of malware, or at least that the Government cannot prove otherwise given the evidentiary mess arising from the FBI's use of malware in the first place. The NIT discovery is therefore material to potential defenses.

While the Government will no doubt continue to disparage those defenses, its assessment of their merit is irrelevant. *See 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 present his theories of defense "even if his evidence is weak, insufficient, inconsistent, or of doubtful credibility") (citation omitted). And, as a practical matter, the position the Government has staked out has created an evidentiary "Catch 22" that will likely foreclose it from trying to rebut the defenses at trial. If the Government tries to call expert witnesses for rebuttal, it may be foreclosed from doing so because the witnesses will have no relevant foundation for their testimony about how the NIT components actually worked.

Alternatively, if the Government allows its experts to analyze all of the components, it will have to allow the same access to defense experts. Otherwise, it will be asking the Court to allow the prosecution to present expert testimony that the defendants will have no meaningful ability to challenge. *See, e.g.*, *Ake v. Oklahoma*, 470 U.S. 68, 82 (1985) (one function of a defense expert is "to assist in preparing the cross-examination" of a State's expert.). Either way, the Government's decision not to provide discovery is a dead end, for all practical purposes making it impossible to present these cases to juries.

II. CONCLUSION

For the reasons stated above and in the defendants' Motion to Exclude, the defendants respectfully request that the Court impose appropriate sanctions for the non-disclosure of material evidence, namely exclusion of all fruits of the NIT searches.

DATED this 17th day of October, 2016.

Respectfully submitted,

s/ *Colin Fieman*
Colin Fieman
Attorney for David Tippens

s/ Robert Goldsmith
Robert Goldsmith
Attorney for Gerald Lesan

s/ Mohammad Hamoudi
Mohammad Hamoudi
Attorney for Bruce Lorente

CERTIFICATE OF SERVICE

I hereby certify that on October 17, 2016, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to all parties registered with the CM/ECF system.

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

A CERTIFIED TRUE COPY
ATTEST: WILLIAM M. McCOOL
Clerk, U.S. District Court
Western District of Washington
By
Deputy Clerk

UNITED STATES DISTRICT COURT

for the
Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

2441 76th Avenue SE, Apt. 524, Mercer Island, WA 98040, and the person of Thomas Stephen Clark, DOB XX/XX/1987

Case No. MJ16-377

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

The residence 2441 76th Ave. SE, Apt. 524, Mercer Island, WA 98040, and the person of Thomas Stephen Clark as further described in Attachment A, which is attached hereto and incorporated herein by this reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, which is attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

☑ evidence of a crime;
☑ contraband, fruits of crime, or other items illegally possessed;
☑ property designed for use, intended for use, or used in committing a crime;
□ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. § 2252 (a)(2)	Receipt and distribution of child pornography
Title 18, U.S.C. § 2252(a)(4) (B)	Possession of child pornography

The application is based on these facts:

See attached Affidavit

☑ Continued on the attached sheet.

□ Delayed notice of ____ days (give exact ending date if more than 30 days: ____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

SCOTT SUTEHALL, SPECIAL AGENT DHS/HSI
Printed name and title

Sworn to before me and signed in my presence.

Date: Aug. 31, 2016

Judge's signature

City and state: Seattle, Washington

MARY ALICE THEILER, U.S. MAGISTRATE JUDGE
Printed name and title

Exhibit A-1

ATTACHMENT B

ITEMS TO BE SEIZED

The following records, documents, files, or materials, in whatever form, including handmade or mechanical form (such as printed, written, handwritten, or typed), photocopies or other photographic form, and electrical, electronic, and magnetic form (such as CDs, DVDs, storage cards, USB flash/thumb drives, camera memory cards, electronic notebooks, or any other storage medium), that constitute evidence, instrumentalities, or fruits of violations of 18 U.S.C. § 2252(a)(2) (Receipt or Distribution of Child Pornography) and 18 U.S.C. § 2252(a)(4)(B) (Possession of Child Pornography), which may be found at the SUBJECT PREMISES, and on the person of THOMAS STEPHEN CLARK:

1. Any visual depiction of minor(s) engaged in sexually explicit conduct, in any format or media;

2. Evidence of the installation and use of APPLICATION A software, any associated logs, saved display or usernames ("C P" and/or "aceofspades05"), email address(es) ("tom.s.clark@gmail.com"), passwords, shared files, and browsing history;

3. Letters, emails, text messages, and other correspondence identifying persons transmitting child pornography, or evidencing the transmission of child pornography, through interstate or foreign commerce, including by mail or by computer;

4. All invoices, purchase agreements, catalogs, canceled checks, money order receipts, credit card statements or other documents pertaining to the transportation or purchasing of images of minors engaged in sexually explicit conduct;

5. Any and all address books, names, lists of names, telephone numbers, and addresses of individuals engaged in the transfer, exchange, or sale of child pornography;

6. Any and all diaries, notebooks, notes, non-pornographic pictures of children, and any other records reflecting personal contact or other activities with minors;

7. Digital devices and/or their components, which include, but are not limited to:

Exhibit A-2

a. Any digital devices and storage device capable of being used to commit, further, or store evidence of the offense listed above;

b. Any digital devices used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, cameras, printers, encryption devices, and optical scanners;

c. Any magnetic, electronic, or optical storage device capable of storing data, such as disks, tapes, CD-ROMs, CD-Rs, CD-RWs, DVDs, printer or memory buffers, smart cards, PC cards, memory sticks, USB flash drives, camera memory cards, media cards, electronic notebooks, and personal digital assistants; d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software;

e. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices, or data to be searched;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data;

8. Evidence of who used, owned or controlled any seized digital device(s) at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, saved user names and passwords, documents, and browsing history;

9. Evidence of malware that would allow others to control any seized digital device(s) such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malware; as well as evidence of the lack of such malware;

10. Evidence of the attachment to the digital device(s) of other storage devices or similar containers for electronic evidence;

Exhibit A-3

completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the computers. To effect such accuracy and completeness, it may also be necessary to analyze not only data storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the computer and software.

VI. SEARCH AND/OR SEIZURE OF DIGITAL DEVICES

38. In addition, based on my training and experience and that of computer forensic agents that I work and collaborate with on a daily basis, I know that in most cases it is impossible to successfully conduct a complete, accurate, and reliable search for electronic evidence stored on a digital device during the physical search of a search site for a number of reasons, including but not limited to the following:

a. Technical Requirements: Searching digital devices for criminal evidence is a highly technical process requiring specific expertise and a properly controlled environment. The vast array of digital hardware and software available requires even digital experts to specialize in particular systems and applications, so it is difficult to know before a search which expert is qualified to analyze the particular system(s) and electronic evidence found at a search site. As a result, it is not always possible to bring to the search site all of the necessary personnel, technical manuals, and specialized equipment to conduct a thorough search of every possible digital device/system present. In addition, electronic evidence search protocols are exacting scientific procedures designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since ESI is extremely vulnerable to inadvertent or intentional modification or destruction (both from external sources or from destructive code embedded in the system such as a "booby trap"), a controlled environment is often essential to ensure its complete and accurate analysis.

Exhibit A-4

UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA
STATESVILLE DIVISION

UNITED STATES OF AMERICA,) DOCKET NO. 5:15-cr-15
)
vs.)
)
STEVEN W. CHASE,)
)
Defendant.)
________________________________)

TRANSCRIPT OF DANIEL ALFIN TESTIMONY
BEFORE THE HONORABLE RICHARD L. VOORHEES
UNITED STATES DISTRICT COURT JUDGE
SEPTEMBER 14, 2016

APPEARANCES:

On Behalf of the Government:

CORTNEY S. RANDALL, ESQ.,
Assistant United States Attorney
227 West Trade Street, Suite 1700
Charlotte, North Carolina 28202
REGINALD E. JONES, ESQ.,
United States Department of Justice
1400 New York Avenue, NW
Washington, DC 2005

On Behalf of the Defendant:

PETER ADOLF, ESQ.,
Federal Defenders of Western North Carolina
129 West Trade Street, Suite 300
Charlotte, North Carolina 28202

LAURA ANDERSEN, RMR
Official Court Reporter
United States District Court
Charlotte, North Carolina

Exhibit B-1

A. Yes, that's what the post says.

Q. Now you were present in court -- you were present in court when Special Agent -- or I'm sorry -- Supervisory Special Agent O'Donnell was on the stand; is that right?

A. Yes, that's correct.

Q. And you recall us talking about what mal-ware is and how it works.

A. Yes, there were questions regarding mal-ware.

Q. And you're aware that -- I guess one of the dangers of going to websites that you're not familiar with, or dangers of opening emails that -- or attachments to emails, in general, that you don't know the source of, is that you can end up with mal-ware on your computer.

A. Mal-ware can be -- you can get mal-ware on your computer through various different ways, including opening malicious email attachments, as you've said.

Q. Or going on websites where there's criminal intent behind the person who's running the website and they're trying to gather information from the people who click on whatever links are on the website.

A. That's possible as well.

Q. And it is possible, in fact, to write mal-ware, to set it up so that somebody who is trying to download an image from a website that's set up to do it, who's trying to open a video or download some other file, can end up with a program on

Exhibit B-2

their computer that takes information from their computer and sends it to someone else without them knowing it?

A. Yes, that's accurate. Mal-ware is generally designed -- if you're going to steal someone's information -- you don't want them to know that it's happening.

Q. And more than them not knowing that it's happening when it happens, programs like that can also be written so that there is no code left behind on the computer, once that information has been sent somewhere else.

A. Yes, that's correct.

THE COURT: Members of the jury, we'll take our afternoon break at this time. I would ask you to keep in mind the usual instructions. Call for you in 15 minutes.

(The jury was escorted from the courtroom at 3:12.)

THE COURT: As always, I urge the parties to take the time they need, but move along as best we can.

MR. ADOLF: Yes, Your Honor.

THE COURT: Thank you.

May we have the jury.

(The jury was returned to the courtroom at 3:32.)

THE COURT: All right. The jury is with us.

MR. ADOLF: Thank you, Your Honor.

Q. Agent Alfin, I'm showing you more data that was produced on Cygnus -- using Cygnus. And I'd like you to take a look through it and see if this reflects all of the log-in data

Exhibit B-3

JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. DAVID TIPPENS, Defendant.	No. CR16-5110RJB DECLARATION OF LEONID REYZIN

I, Leonid Reyzin, declare under penalty of perjury that:

1. I am a Professor of Computer Science at Boston University. I specialize in network security and cryptography. I am also a member of the Boston University Security Group, and the Boston University Center for Reliable Information Systems and Cyber Security. A copy of my *curriculum vitae* is attached to this declaration.

2. I have communicated with the Federal Public Defender in Boston in connection with an "Operation Pacifier"/ NIT case pending there. I was introduced to Colin Fieman, counsel for Mr. Tippens, during a conference call related to that case. Mr. Fieman asked if I would be willing to review the expert declarations that have been submitted in connection with his client's case and offer an opinion about the technical issues that are addressed in them. I agreed to do that and have reviewed the declarations of Prof. Brian Levine, Vlad Tysrklevitch, Prof. Matthew Miller, Shawn Kasal and digital forensic specialist Robert Young.

Exhibit C-1

3. I am providing this declaration *pro bono*, without compensation or a connection to either party through research funding or grants.

4. I endorse the declarations that have been submitted to the Court by the defense experts. In my opinion, they correctly state the need for disclosure of all the NIT components, particularly the "exploit" component, and the challenges facing the defense if they do not have an equal opportunity to examine the components.

5. Without getting bogged down in highly technical details, there are several basic, common sense problems with the expert opinion that has been submitted by the Government. First and foremost, while Prof. Levine has a solid grasp of how "network techniques" are *supposed* to operate if they are programmed and deployed correctly, he states that he has not analyzed any of the relevant components. Instead, he relies extensively on assertions from an FBI Agent who, I am informed by defense counsel, has not examined the components either. It does not take any specialized training or expertise to realize that this is not a scientifically sound basis for rendering an opinion.

6. As a result, it appears that Prof. Levine does not have sound factual support for key conclusions. For example, at the end of paragraph 4 of his declaration, he states: "The exploit and payload did not persist on the defendants' computers after execution." A careful reading of the entire declaration establishes that the only apparent basis for this statement is Agent Daniel Alfin's conclusion to the same effect.

7. Professor Levine's declaration also contains a glaring self-contradiction: on the one hand, he states (in ¶4) that the "exploit and payload did not persist on the defendants' computers after execution." On the other hand, he claims multiple times that the defense would be able to find other malware "through an examination of the defendants' computers" (¶10; similarly in ¶¶ 12, 17 and 19). But if the FBI's malware (NIT) was able to "not persist" on the computers, then other malware also, of course,

has the same capability, and the examination of the defendants' computers would turn up no traces of it.

8. Moreover, since the defense experts do not have access to all of the information they are seeking, it does not make sense to fault them for not offering direct evidence to support their opinions. Their declarations do offer substantial factual support for their opinions, based on well-documented instances of the vulnerabilities and damage that NIT-type malware can cause. In my view, Prof. Miller, Vlad Tysrklevitch and Shawn Kasal are particularly well qualified to render opinions on NIT issues given their work with the type of malware and code analysis at issue in this case.

9. The defense, in its reply to Prof. Levine's declaration, also accurately summarizes multiple defects in the Government's assertions and Prof. Levine's descriptions, among other things, of how the Tor network operates and the centrality of the "exploit" component to the issues in these cases.

10. I am not a digital forensics expert, but I am also in agreement with the opinion of Robert Young that it is not feasible to "reverse engineer" the NIT components or their effect on targeted computers by analyzing the data contained on a copy of the defendants' hard drives or other storage devices. As a practical matter, trying to find the relevant data would not only be like looking for a needle in a haystack, but looking for a needle that may have been hidden, encrypted or already deleted. A reliable forensic analysis is further complicated by the fact that there is reason to believe that the agents who seized the defendants' computers may not have followed the usual protocols for preserving the data on those computers.

Dated: October 17, 2016

Leonid Reyzin

Leonid Reyzin, PhD.

Exhibit C-3