The Honorable Robert J. Bryan

UNITED STATES DISTRICT COURT FOR THE
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. DAVID TIPPENS, Defendant.	NO. CR16-5110 RJB GOVERNMENT'S RESPONSE TO MOTION TO EXCLUDE (Evidentiary Hearing Requested)
UNITED STATES OF AMERICA, Plaintiff, v. GERALD LESAN, Defendant.	NO. CR15-387 RJB GOVERNMENT'S RESPONSE TO MOTION TO EXCLUDE (Evidentiary Hearing Requested)
UNITED STATES OF AMERICA, Plaintiff, v. BRUCE LORENTE, Defendant.	NO. CR15-274 RJB GOVERNMENT'S RESPONSE TO MOTION TO EXCLUDE (Evidentiary Hearing Requested)

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

I. INTRODUCTION

Defendants have jointly moved to exclude all evidence derived from the government's court-authorized use of a Network Investigative Technique ("NIT") to obtain their IP addresses and other limited information about their computers, while they accessed the illicit Playpen child pornography website via the Tor network. In support of their motion, they ask the Court to rely upon the same information submitted in *United States v. Michaud*. In light of new information presented in the accompanying declaration, and the facts of each case, this Court should deny Defendants' motions and not simply adopt the order that was entered in *Michaud*.[1]

Since the Court's decision in *Michaud*, three other courts have denied nearly-identical motions to compel filed in other cases arising from the same investigation. *See United States v. Darby*, No. 16-cr-036 (E.D. Va. Aug. 12, 2016) (attached as A-11) (finding defendant's claims of materiality to be speculative, the requested information immaterial, and that the law enforcement privilege properly shielded the requested information from disclosure); *United States v. Matish*, No. 4:16-CR-16, 2016 WL 3545776 (E.D. Va. June 23, 2016) (same); *see also United States v. Eure*, No. 2:16-CR-43, 2016 WL 4059663 (E.D. Va. Aug. 15, 2016) (incorporating *Darby*).[2] These motions were filed after the defense in each case was provided with access to the exact same information that has been made available to the defendants in these cases.

With this response, the government submits the declaration of Professor Brian Levine, a Ph.D. in Computer Engineering and the Director of the University of Massachusetts Amherst Cybersecurity Institute. Professor Levine has reviewed the same

---

[1] Like Defendants and for the sake of brevity, the government incorporates by reference pleadings from *United States v. Michaud* related to the third motion to compel (Dkt. 134, 156-57), the request for reconsideration of the order on that motion (Dkt. 165-66, 187-88), and the memorandum regarding appropriate sanctions (Dkt.207) This response will focus on the new information available to the Court.

[2] In *Matish*, the defendant submitted the Tsyrklevich declaration from the *Michaud* case, a declaration by Matthew Miller, a declaration by Christopher Soghoian, and this Court's order from the *Michaud* case. In *Darby*, the defendant submitted the Tsyrklevich declaration from the *Michaud* case. In *Eure*, decided by the same judge as in *Darby*, the defendant submitted the Tsyrklevich declaration from the *Michaud* case, a declaration from Matthew Miller, a declaration from Christopher Soghoian, and testimony from Dr. Soghoian.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

information available to the Defendants in this case. His declaration substantially clarifies and refutes the wildly speculative claims littered throughout the defendants' expert declarations, which are not supported by any evidence. The declaration confirms that review of the information that the defense seeks is neither material nor necessary in order to raise or evaluate their defenses. For these and the other reasons outlined below, Defendants' motion should be denied.

II. BACKGROUND

Each of the defendants was a registered user of the Playpen child pornography website, which operated on the anonymous Tor network. The defendants were identified after each of their home IP addresses were recorded accessing Playpen during the brief time it was under FBI control through the use of the NIT. In each case, the FBI obtained a separate warrant to seize and search electronic devices from the defendants' homes, relying, in part, on the IP address identified through the NIT. The FBI then executed search warrants at each Defendant's residence and seized digital devices containing child pornography, along with other evidence. Lorente and Tippens also confessed to having downloaded child pornography over the Internet. Lesan made similarly incriminating statements in emails to his estranged wife that he sent following the search of his home.

Each Defendant has been provided access to substantial discovery pertaining to the FBI's use of the NIT to obtain his IP address. That information includes the computer code that was sent to their computers and executed, which produced the NIT results (referenced as the "payload"); the NIT results – i.e., the IP address and other computer-related information the FBI obtained via the NIT; a two-way data stream ("PCAP" data) documenting the data sent between their computers and the government's computer as the NIT executed. Most importantly for purposes of the crimes with which Defendants are charged, they have access to all of the devices that were seized from their homes and on which the child pornography they are charged with possessing and receiving was found.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

III. ARGUMENT

A. Defendants have not shown the information they seek is material under Rule 16 because their claims rest upon theoretical, speculative concerns unsupported by facts.

Under Rule 16, a criminal defendant has a right to inspect documents, data, or tangible items within the government's "possession, custody, or control" that are "material to preparing the defense." Fed. R. Crim. P. 16(a)(1)(E). Evidence is "material" under Rule 16 only if it is helpful to the development of a possible defense. *United States v. Olano*, 62 F.3d 1180, 1203 (9th Cir. 1995). "[I]n the context of Rule 16 'the defendant's defense' means the defendant's response to the Government's case in chief." *United States v. Armstrong*, 517 U.S. 456, 462 (1996).

In order to compel discovery under subsection (a)(1)(E), a defendant must make a "threshold showing of materiality." *United States v. Santiago*, 46 F.3d 885, 894 (9th Cir.1995). "Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present *facts* which would tend to show that the Government is in possession of information helpful to the defense." *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990) (emphasis added). "[O]rdering production by the government without any preliminary showing of materiality is inconsistent with Rule 16." *Mandel*, 914 F.2d at 1219. In fact, "[w]ithout a factual showing there is no basis upon which the court may exercise its discretion, and for it to ignore the requirement is to abuse its discretion." *Mandel*, 914 F.2d at 1219. Moreover, Rule 16 "does not authorize a fishing expedition." *United States v. Rigmaiden*, 844 F. Supp. 2d 982, 1002 (D. Ariz. 2012).

As detailed below, the defendants' motion consists of nothing more than a demand for a "fishing expedition." The defendants raise theoretical concerns about the capabilities of exploits and the possibility of errors in generating unique identifiers. The government has presented sworn testimony stating that the NIT did not collect additional information beyond what was authorized; that the exploit used did not make permanent

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

changes to the security settings of Defendants' computers; and that all the unique identifiers generated during the operation were unique. Defendants counter that they should not be required to accept the government's word as to those points. But in order to be granted discovery on these points, they must proffer some fact that suggests that the theoretical problems they fear actually manifested themselves and that if they did, that they would be relevant to the crimes with which they are charged. Despite access to the computer code and the devices on which the evidence was found, they have yet to offer any concrete evidence to support the speculative claims, or any facts gleaned from a review of this evidence that would support these speculations. Indeed, even taking their declarations at face value, they fail to do so. That should be fatal to their claim of materiality. As the Court in *Darby* explained:

> Defendant invents a variety of scenarios whereby the information he seeks about the operation of the NIT might aid him in developing a defense. Defendant has not used any of the information that the government has provided to him or offered to provide him in order to establish a factual basis for these scenarios. As a result, the Court does not have before it any evidence that the information sought would aid this Defendant. Furthermore, the scenarios, mostly, are not drawn to any particular feature of the NIT used by the government and would apply to any NIT deployed by means of an exploit. In short, all Defendant places before the Court are stories about how a generic defendant located by means of a generic NIT might need the information sought in order to develop his or her defense. This is not enough to require disclosure . . . .

Darby, A-11 at 8.[3]

[3] The Fourth Circuit's standard for the showing a defendant must make in order to demonstrate materiality is derived from Ninth Circuit law. *See United States v. Caro*, 597 F.3d 608, 621 (4th Cir. 2010) ("[n]either a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense")(quoting *Mandel*, 914 F.2d at 1219). The definition of materiality in the Fourth Circuit is similar, if more specifically defined, to that of the Ninth Circuit. *See Id.* (evidence material where there is "some indication that the pretrial disclosure of the disputed evidence would have enabled the defendant significantly to alter the quantum of proof in his favor" and "as long as there is a strong indication that it will play an important role in uncovering admissible evidence, aiding witness preparation, corroborating testimony, or assisting impeachment or rebuttal.").

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

In any event, as now revealed by the declaration of Professor Levine, the defendants' expert declarations are replete with "overbroad generalizations and implausible explanations" that are "not rooted in cited or documented facts or evidence" and which are "insufficient to support their hypotheses." Levine Dec. at 4, ¶ 6. Upon his review of the same information available to the Defendants, Professor Levine has concluded that there is "no evidence to support any . . . hypotheses referenced in the defendants' submissions" suggesting that NIT information was "tampered with or altered," that "identifiers generated by the FBI are not reliable," that the "FBI exploit or payload made permanent changes to the security settings or any other settings of the defendants' computers" or that any "FBI exploit or payload are responsible for images of child sexual abuse found on the defendants' computers and in their residences." *Id*. Moreover, Professor Levine concluded that reviewing the FBI's exploit, software that generated unique identifiers, or server software – as opposed to reviewing the defendants' computers – is "not necessary to show that these hypotheses are merely speculation premised upon extremely unlikely theoretical possibilities." *Id*. at 4-5, ¶ 6.

Because the defendants' claims are premised on speculation, not fact, their motion should be denied.

1. The NIT-derived information is tangential to the government's proof at trial.

Evaluating the materiality of the requested discovery first requires a clear understanding of the evidence obtained through the NIT[4] and through the subsequent execution of search warrants at Defendants' homes. The NIT warrant authorized the collection of discrete information, including an IP address, a MAC address, and

[4] Although Defendants define the NIT to include every aspect of obtaining information from the computers connecting to Playpen as a result of the Eastern District of Virginia warrant, the government has not characterized the term as such. Indeed, that is obvious from the Eastern District of Virginia warrant. A warrant is required for a Fourth Amendment intrusion. Thus, for purposes of issuance of a warrant, except for night time execution or whether the agents may execute without knocking, it is irrelevant if the agents travel to or even how they gain entry to a residence to execute a warrant. What was authorized by the Eastern District of Virginia warrant was deployment of computer code (or NIT) on computer or other devices connecting to Playpen, in order to obtain the IP addresses and other information necessary to identify the user.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

information related to the operating system and user account. The evidence supporting the charges against Defendants, in contrast, derives from the residential search warrants executed at their homes and the digital devices seized as a result. These residential search warrants relied on the IP address information obtained by the NIT to be sure, but the actual evidence of the charged offenses comes not from the NIT but the devices obtained from and statements made by Defendants. This distinction is meaningful because Defendants' discovery demands go not to the core of the evidence that will form the basis of the government's proof at trial but rather the investigative technique that led to their identification.

2. Defendants point to no facts in support of their speculative concerns about whether the NIT collected additional information, made permanent changes to their computers, or failed to generate unique identifiers.

Though offering slightly different formulations at points, Defendants and their experts offer two primary theories of materiality, neither of which hold up to scrutiny. First, they say they must verify the accuracy of the information collected by the NIT and ensure that the NIT did not exceed the scope of the authorizing warrant. Second, they say that absent this discovery, they cannot effectively evaluate the viability of a defense premised on the theory that someone or something else was responsible for the child pornography found on their computers. Beyond saying it is so, however, neither Defendants nor their experts cite any fact to suggest that the NIT information was inaccurate or that someone or something else was responsible for child pornography on their devices. And as explained below and in the declarations of Professor Levine and Special Agent Daniel Alfin, reviewing the requested information will not advance their cause.

a. Defendants present no facts to suggest that the NIT data is inaccurate and have the ability to verify its accuracy with current discovery.

First, as to the accuracy of the NIT data, Defendants point to not one scintilla of evidence to suggest that the NIT data were, in fact, inaccurate. Rather, they simply make

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the obvious assertion that it is always *possible* that data could be inaccurate. But suggesting a possibility, no matter how remote, is not enough to establish materiality.

Moreover, Defendants' have been given all of the information necessary to confirm the accuracy of the information collected by the NIT. Defendants and their experts have access to (1) the computer code that actually performed the search of their computers, (2) the results of that search, (3) the network data stream that documents the transmission of those search results from Defendants' computers to the FBI; and (4) their computers and digital devices. As the court in *Darby* found, "Defendant's concerns about the operation of and data collected by the NIT have been addressed by these disclosures." *Darby*, A-11 at 10. Their supposed inability to verify the accuracy of the NIT search results is a problem of their own creation. Rather than review the available information and follow it where it leads, Defendants prefer conjecture about all the ways in which those results could have been recorded incorrectly, tampered with, or corrupted. Tellingly, however, they cannot point to anything that would suggest this actually happened.

The work of Professor Levine, however, shows that Defendants' conjecture about errors in the data is just that and that the discovery they request will get them no closer to evidence that would support their speculation. Unlike Defendants and their experts, Professor Levine—an expert in network protocols and cybersecurity—has looked at the available information, including the network data. Using that same information that the defense has chosen not to review and rely upon, Professor Levine explained that the evidence leaves him confident that the information collected by the NIT was reliably and accurately transmitted and stored by the FBI. Levine Dec. at 11-16, ¶¶ 21-31. For instance, his examination of packet capture ("PCAP") data made available to the defendants, but which they have so far declined to analyze, showed that the NIT information "was returned accurately to FBI servers." *Id*. at 11, ¶ 22.

He likewise explains in detail why Defendants' misgivings about the lack of encryption are a red herring because of "other protections that were in place, the realities

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

of the Internet, and the facts of this case." *Id*. at 11, ¶ 22. Specifically, the connection between the Defendants' computers and the government computer to deliver the NIT information involved a type of data exchange that "occurs many billions of times per day on the Internet," and Professor Levine's review of the data available to the Defendants showed "nothing out of the ordinary." *Id*. at 12-13, ¶ 24. Based on his review of information returned by the defendants' machines to the FBI, Professor Levine also found that internal "checksums" – used to ensure a lack of errors in data transmission – were valid. *Id*. at 13, ¶ 26. Were they not, he reported in common-sense terms, data could not have been properly routed back-and-forth, similar to how one cannot exchange letters via U.S. Mail if the envelopes contain wrong addresses. *Id*. at 14, ¶ 27.

Moreover, Professor Levine described how the likelihood that the data sent by the NIT was corrupted (intentionally or inadvertently) is exceedingly low. *Id.* at 11-15, ¶¶ 21-28. In order for that to be the case, some nefarious actor would have needed "voluminous, non-public information about the FBI's investigation and each of the defendants' computers," access to Internet infrastructure, and sophisticated malware. *Id.* at 15, ¶ 29. Defendants point to no facts suggesting that was the case. Finally, he rebutted any suggestion that Defendants need access to the government's server(s) to conduct the analysis he performed, when they can examine the data recorded by the government and the network traffic sent by the NIT. *Id.* at 16, ¶¶ 29-30. Simply put, information in the FBI's server logs would be redundant of the packet capture information made available to the defense. *Id*. at 16, ¶ 31.

b. Defendants present no facts to suggest that the NIT or exploit exceeded the scope of the authorizing warrant or made permanent, damaging changes to their computers, and have the ability to verify the NITs accuracy with current discovery.

For the same reason, Defendants have available to them everything they need to confirm that the NIT did not exceed the scope of the authorizing warrant. As Professor Levine notes, the evidence shows that the payload sent to Defendants' computers operated to collect the information authorized by the NIT warrant. Levine Dec. at 11, ¶

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

21. Defendants counter that without the exploit, they cannot be certain that the government did not deploy some additional payload or other code capable of going beyond what was authorized in the NIT warrant. This argument, however, is premised entirely on unfounded speculation that the government misrepresented what it seized from the defendants' computers. The government has provided in discovery the only information collected via the NIT. Other than to note that it is possible, Defendants point to no evidence that the government seized something else or that anything in the computer code or found on the devices suggests otherwise. And even if additional information had been collected, which it was not, such information would clearly be subject to suppression.

Defendants and their experts have offered a litany of things the exploit *could* have done to Defendants' computers separate and apart from seizing additional or unauthorized information. But that also gets them nowhere. For starters, as Professor Levine notes, while the expert declarations are long on hypotheses, they are woefully short on evidentiary support for their theories. Levine Dec. at 5-11, ¶¶ 9-20. Indeed, they devote considerable ink to all the things the exploit could have done to the Defendants' computers. Yet they are silent when it comes to explaining what support they have found for their theories in the one place one might expect—the Defendants' computers. *Id.*

As Professor Levine points out, while the defendants' experts speculate about exploits that might cause a computer to crash or lose or alter data or adjust the security settings on defendants' computers, such "speculation is not supported by any information in the defendants' submissions that shows that any defendants' computers actually experienced any of those symptoms." *Id*. at 6, ¶ 9. Moreover, he would have expected that statements claiming such possibilities "would be based on evidence that resulted from an examination of the defendants' computers and devices demonstrating" that one of those conditions actually occurred. *Id.* This is perhaps all the more surprising because as Professor Levine observes, the defendants' experts are:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

> clearly qualified to find evidence of malware, examples of settings that suggest malware, evidence of tampering, examples of data incongruities that begin to suggest tampering, etc. None have been found. All can be found without review of the exploit, but without such findings from the defendants' computers, specific supporting analysis, or other evidence, their declarations offer not more than speculation and general possibilities rather than sound conclusions.

Id. at 10, ¶ 17.Other courts confronted with similarly broad but utterly unsupported assertions about all the harm that the government's use of the NIT could have wrought have been similarly unimpressed. As the court in *Matish* found:

> the purposes for which Defendant asks for access to the missing source code are based upon speculation as to what the declarants might find. The defense lacks any evidence to support the hypotheses and instead relies upon the *ipse dixit* that the source code is needed because its declarants opine that it is needed. Such speculation remains insufficient to serve as a basis to compel discovery.

2016 WL 3545776 at *6. *Darby* offered a similar sentiment:

> Defendant also argues the he needs to examine the code for the exploit because the exploit might have altered the security features of his computer. Other individuals might then have placed child pornography on his compromised computer. Again, Special Agent Alfin has stated in his declaration that the exploit does not weaken the security features of the computers against which it is deployed. Again, Defendant says that he should not have to rely on the assurances of government agents. Again, Defendant submits no evidence that the security features of his computer were altered. The government has offered Defendant the opportunity to inspect his computer for signs that its security features were compromised and for signs that it was later hacked. Defendant still presents no evidence in support of his hypothetical. Absent in evidence in support of his hypothetical, he is not entitled to disclosure of the exploit.

A-11 at 11 (citations omitted).

Nor, more importantly, would defendants' review of the exploit be helpful given their purported need. More precisely, examination of the exploit would explain *how* the NIT actually was delivered to their computers but would tell them nothing about *what* the NIT did once there and what information was sent to the government. Levin Dec. at 6-7, ¶ 10. As Professor Levin explains:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

> an examination of the exploit to determine how or if settings were changed, regardless of the outcome, would not shed light on whether some third-party actor delivered child pornography to a defendant's computer. The defense would need to search for evidence of malware, which they can do through an examination of the defendants' computers. Computers are always vulnerable to threats known and unknown, just as someone's home is always vulnerable to a break-in. Looking at a lock to determine whether it is broken, or can be picked, does not and cannot tell the homeowner what someone who might have broken or picked the lock did after entering the house. Similarly, reviewing one particular exploit would provide evidence that a defendant's computer was vulnerable to that one particular exploit, but it would shed no light upon the computer's potential vulnerabilities to innumerable others. Nor would it shed any light on what particular malware was or could have been delivered to that computer. Reaching that conclusion requires an examination of the computer.

Id.

Put another way and in terms the Court has used previously, discovery about the exploit could identify *one* means by which someone could have "hacked" Defendants' computers but says nothing about whether they were actually "hacked" or what happened after. Indeed, discovery about the exploit would identify only a single vulnerability by which those devices could have been compromised, not every potential security weakness that may have exposed them to such attacks. And the "first reasonable place to look" for evidence of a hack, and evidence of what the hack did to your computers and devices, is your computers and devices. *Id*. at 7, ¶ 11. Defendants point to no evidence that they have even attempted such an analysis, let alone evidence that such an analysis showed some sort of malware that was or could be attributable to the FBI.

c. Defendants present no facts to suggest that there were any errors with unique identifiers, which current discovery has verified.

Finally, the suggestion that there might be some error in the creation of the unique identifiers used to track the NIT results from individual computers to which it was deployed does not demonstrate the need to know the manner in which the NIT instructions were delivered. In a declaration under oath, the government has affirmed

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

that it has reviewed the unique identifiers generated during this investigation and confirmed that they were in fact unique. Ex. 5, Declaration of Special Agent Daniel Alfin, *United States v. Matish*, No. 16-cr-016, Dkt 74-1 at 5, ¶¶ 24-27. On the issue of the unique identifiers, then, the government is in possession of no information that would be helpful to the defense. Moreover, the defendants have presented no facts to suggest otherwise – only unsupported conjecture. That does not entitle them to discovery. *See Mandel*, 914 F.2d 1215, 1219 ("defendant must present *facts* which would tend to show that the Government is in possession of information helpful to the defense."); *see also Darby*, A-11 at 10 ("Defendant has put forth nothing but speculation that such duplicates might have existed. This is not enough . . . to mandate disclosure by the government."). And while Defendants again make much of the possibility that an error might have occurred, Professor Levine explained in detail why Defendants' conjecture on this point is just that. Levin Dec. at 16-19, ¶¶ 31-37. As he explains, where, as here, the "entire exchange between the defendants' computers and the FBI server was completed in under 1 second," he places the odds that any two pairs of identifiers would be duplicates at "less than 1 in 1,000,000,000,000." *Id*. at 17, ¶¶ 35-36.

d. Defendants fail to point to facts to show that the information sought is relevant and helpful to evaluate a malware defense.

Moreover, even if there were something to Defendants' concerns, they relate only to the question of whether there was probable cause to support the warrant authorizing the search of their homes. And unless any such defects were obvious, the warrant would still stand, since the IP address directly tied to Defendants' homes, and the evidence seized as a result remains available for trial.

Defendants also say that the additional discovery is necessary because someone or something else could be responsible for planting the child pornography found on their devices. To support this claim, they offer only a whole host of scenarios by which deployment of the NIT *could* have left their devices vulnerable to intrusion and why only additional information, including the exploit, will suffice to allow them to fully

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

investigate the matter. As a threshold matter, no one disputes that computers are vulnerable to intrusion. That was true before the NIT was deployed, and it was true after. To be sure, someone or something could have exploited that same vulnerability (or some other one) and could theoretically have planted child pornography on their devices. The defendants' declarations amply prove that obvious point.

Although they had access to the devices that would contain the evidence of such malware, the defendants have failed to point to any evidence that their computers or devices were actually subject to that sort of exploit or malware. Absent that, they present no fact to justify discovery on this point. And as Professor Levine's declaration makes abundantly clear, their computers and devices is where one would expect to look in order to find that sort of evidence. Defendants point to no such evidence.

If the question Defendants seek to answer is not whether they could have been victims of malware (they could), but to evaluate the strength of a defense premised on the theory that they were victims, they continue to have what they need at their disposal. In addition to reviewing their own computers for malware and security vulnerabilities, each defendant can assess the state of the evidence that had nothing to do with the NIT deployed here. For instance, each defendant made incriminating statements that would make presenting such a defense challenging under the best of circumstances. Lorente and Tippens both confessed to a long-term habit of downloading child pornography when confronted by law enforcement. CR15-274RJB Dkt 1 at 6, ¶ 15 (Lorente Complaint); CR16-5110RJB Dkt 1 at 5-6, ¶ 11 (Tippens Complaint). Tippens was actually watching a child pornography video when police entered his home. *Id.* at 5, ¶ 10. And Lesan, though he did not confess to law enforcement, made incriminating statements to his estranged wife, including acknowledging the creation of voyeuristic videos that showed nude minors and adults. *See* Ex. 6. It is of course not for the Court to decide whether any particular defense would be successful at this stage in the game, but it is certainly relevant to the determination of materiality – on the basis of a need to evaluate the merits

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

of a potential malware defense – that Defendants already have a substantial volume of information that could inform their analysis about the viability of this "virus" theory.

More to the point, if Defendants' truly wish to determine whether someone or something else is responsible for the child pornography found in their homes, wouldn't the best place to search for that evidence be the devices themselves? That is clearly the conclusion drawn from Professor Levine's analysis. Despite having access to the devices themselves, their contents, and the NIT computer instructions, however, Defendants present not a shred of evidence to support their theory. They have not even, so far as the government is aware, attempted to examine the devices. And they instead insist further discovery related to the method of deployment of the NIT is critical to evaluating the viability of this theory.

The simple analogy referenced by Professor Levine proves useful. An exploit can be thought of as a tool used to open a locked door. Levine Dec. at 3, ¶ 4. Imagine a conventional search of a defendant's home: Law enforcement picks a locked door in order to enter the home and then seize evidence from the home. First, knowing the method that law enforcement used to pick the lock when it entered sheds no light on what evidence the government seized after it entered. Second, anyone who knows any method of picking a lock could have also picked the lock (and "planted" evidence). Knowing how law enforcement picked the lock therefore offers no insight into the likelihood that someone else did so. Third, if the defendant's concern is that law enforcement picked, and broke, the lock (and left it unrepaired), such that someone could have come in afterwards without needing to pick the lock (and "planted" evidence), it is still immaterial to know *how* law enforcement picked the lock. The material issue there is – is the lock broken – so that anyone could have entered (and "planted" evidence) even if they didn't know how to pick the lock. Resolving that question simply requires the defense to examine the lock – i.e., their computers and devices – not how law enforcement picked it.

To be sure, Defendants need not agree with Professor Levine's amply supported, sound conclusions. But his review starkly highlights the fact that their wildly speculative

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

claims are wholly overblown and unsupported by any actual facts, and that they are capable of doing the sort of verification and evaluation that they seek to conduct with the discovery currently available.

B. Even if the requested discovery is material under Rule 16, it is shielded from discovery by a qualified law enforcement privilege.

Even if the Court believes that disclosure of some or all of the information requested by Defendants is required under Rule 16, a qualified law enforcement privilege applies to bar disclosure because divulging the requested information would be harmful to the public interest. The government thoroughly briefed this issue in its incorporated *Michaud* pleadings. In addition, the government requests the same opportunity granted by the Court in that case to provide a written submission *ex parte, in camera* so it can more fully describe the nature of the information Defendants are seeking and why the government is unwilling to disclose it, even under a strict protective order. As will be explained in more concrete terms in the government's *ex parte, in camera* submission, the public interest in nondisclosure here significantly outweighs Defendants' need for the information, particularly in light of the flimsy showing of materiality they have made. *See also Darby*, A-11 at 11; *Matish*, 2016 WL 3545776 at *8-9 (finding law enforcement privilege applied to bar disclosure of same information requested herein).

C. Should the Court decide sanctions are required, sanctions short of suppression of evidence will cure any potential prejudice Defendants may suffer.

Sanctions short of exclusion of all evidence seized from Defendants' homes will adequately remedy any prejudice Defendants' may suffer as the result of nondisclosure. As stated in the government's pleadings in *Michaud*, this Court is not required to impose any sanction in the event the court determines here that the government is not required to turn over the additional information requested, and the government's position is that none should be. In the event the Court, while balancing the legitimate government and defense interests involved, determines that some sanction is nonetheless appropriate, something far short of suppression of the evidence seized from Defendants' homes should suffice.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

The government has asserted a privilege against disclosure in good faith. Absent findings of bad faith or willfulness combined with a desire to obtain a tactical advantage, even exclusion of evidence would be legally excessive. And as discussed in the *Michaud* pleadings, the Court has appropriate alternatives available. The discovery Defendants seek is at most tangential to the charges and through appropriate crafting of instructions and limits on the evidence available for use by the government can be rendered wholly irrelevant. More important, Defendants have everything they need to evaluate and mount their chosen defense. Finally, the effect, if any, on the jury from the absence of the evidence can be easily addressed through instructions and limitations crafted by the Court. Accordingly, any prejudice defendants may suffer would be minimal, and even that could be cured by an adverse instruction should the Court deem it necessary.

IV. CONCLUSION

For all the foregoing reasons, the Court should deny Defendants' motion to exclude evidence.

DATED this 22nd day of September, 2016.

Respectfully submitted,

ANNETTE L. HAYES
United States Attorney

/s/ Matthew P. Hampton
Matthew P. Hampton
Assistant United States Attorney
1201 Pacific Avenue, Suite 700
Tacoma, Washington 98402
Telephone: (253) 428-3800
Fax: (253) 428-3826
E-mail:
matthew.hampton@usdoj.gov

STEVEN J. GROCKI
Chief

/s/ Keith A. Becker
Deputy Chief
Child Exploitation and Obscenity Section
1400 New York Ave., NW, Sixth Floor
Washington, DC 20530
Phone: (202) 305-4104
Fax: (202) 514-1793
E-mail: keith.becker@usdoj.gov

CERTIFICATE OF SERVICE

I hereby certify that on September 22, 2016, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the attorney(s) of record for the defendant.

s/Emily Miller
EMILY MILLER
Legal Assistant
United States Attorney's Office
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Phone: (206) 553-2267
FAX: (206) 553-0755
E-mail: emily.miller@usdoj.gov