The Honorable Robert J. Bryan

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

UNITED STATES OF AMERICA, Plaintiff v. JAY MICHAUD, Defendant.	NO. CR15-5351RJB **DECLARATION OF FBI SPECIAL AGENT DANIEL ALFIN IN SUPPORT OF GOVERNMENT'S MOTION FOR RECONSIDERATION**

I, Daniel Alfin, declare as follows:

1. I am a Special Agent of the Federal Bureau of Investigation. I am currently assigned to FBI Headquarters, Criminal Investigative Division, Violent Crimes Against Children Section, Major Case Coordination Unit. My duties involve the investigation of individuals using various types of technology to produce, distribute, and trade child pornography. As an Agent assigned to the FBI Violent Crimes Against Children Section, Major Case Coordination Unit, I routinely analyze network data that has been collected pursuant to court order. I hold a University Degree in Information Technology and multiple industry certifications that are recognized by the United States Department of Defense. Additionally, I have completed all stages of FBI Cyber Training including courses on Advanced Network Investigative Techniques, Network Traffic Analysis, Ethical Hacking, and Malware Analysis. Analysis of network data generally consists of

identifying the origin, destination, and content of communications that are sent across the Internet. In addition to performing this type of analysis, I am routinely called upon to assist Agents across the FBI with similar analysis. In the past two years, I have analyzed data from more than 30 court-authorized network intercepts and those analyses have been used in affidavits and court filings in several judicial districts.

2. I have been involved in the FBI investigation of the Playpen website since it came online in approximately August 2014. Playpen was a website that existed on an anonymous network and was dedicated to the advertisement and distribution of child pornography. My duties included the review of Playpen's content on multiple occasions, engagement in undercover activities on Playpen, and the coordination of investigative activity aimed at identifying members of Playpen, including the defendant, Jay Michaud.

3. In preparing this declaration, I have reviewed evidence and spoken with FBI personnel familiar with the facts and circumstances outlined below. I provide the following summary of the information I have learned as a result.

4. I have also reviewed the declaration of Mr. Tsyrklevich, the defense expert, dated January 13, 2016 (Dkt. 115-1, hereinafter "Tsyrklevich Declaration") and noted a number of statements that are inaccurate and/or require clarification. I will address several of these in great detail below but will begin by noting one overarching misconception in that declaration. Specifically, Tsyrklevich attempts to redefine the NIT as something containing multiple components. The NIT, however, consists of a single component—that is, the computer instructions delivered to the defendant's computer after he logged into Playpen that sent specific information obtained from his computer back to the FBI.

A. Disclosure of the "exploit" would do nothing to shed light on whether the government exceeded scope of the NIT warrant.

5. Tsyrklevich claims that he requires access to the government's "exploit" to determine if the government "executed additional functions outside the scope of the NIT warrant." Tsyrklevich Declaration ¶ 6. He is wrong. Discovery of the "exploit" would

do nothing to help him determine if the government exceeded the scope of the warrant because it would explain how the NIT was deployed to Michaud's computer, not what it did once deployed.

6. As used here, a computer "exploit" consists of lines of code that are able to take advantage of a software vulnerability. In layman's terms, an "exploit" could be thought of as a defect in a lock that would allow someone with the proper tool to unlock it without possessing the key. Here, an "exploit" allowed the FBI to deliver a set of instructions—the NIT—to Michaud's computer. Those instructions then gathered specified information, including Michaud's IP address, and transmitted that information to government controlled computers. The NIT instructions have been provided to the defense for review; the "exploit" has not.

7. Because what Tsyrklevich refers to as the "exploit" merely enabled the government to bypass the security protections on Michaud's computer to deliver the NIT instructions, any disclosure about the "exploit" would say nothing about what happened once the NIT instructions were on Michaud's computer. To continue with the lock analogy, knowing how someone unlocked the front door provides no information about what that person did after entering the house. Determining whether the government exceeded the scope of the warrant thus requires an analysis of the NIT instructions delivered to Michaud's computer, not the method by which they were delivered.

B. The unique identifiers were in fact unique.

8. Tsyrklevich maintains that he needs access to the computer code that "generates the payload and injects an identifier" in order to ensure the identifier used was in fact unique. Tsyrklevich Declaration ¶ 5. He is wrong because the unique identifier assigned to Michaud's NIT results was in fact unique.

9. Prior to deployment of the NIT, a unique identifier is generated and incorporated into the NIT. When the "activating computer" sends information to the government as a function of the NIT, that unique identifier is included with the response. When the information is received by the government, a check is performed to ensure that

the unique identifier contained within the delivered information matches the unique identifier that was generated by the government. In the matter at hand, all identifiers received by the government, including the one sent by Michaud's computer, did match identifiers that were generated by the government and they were in fact unique.

10. The ultimate question posed by Tsyrklevich is not how the unique identifier was generated but if the unique identifier sent to Michaud's computer was actually unique. I have reviewed the list of unique identifiers generated during the operation and confirmed that there were in fact no duplicate identifiers generated.

C. Discovery concerning the "server component" is unnecessary because there are alternative means of verifying the accuracy of the NIT information.

11. Tsyrklevich claims that he needs access to the server component in order to confirm that the information obtained from Michaud's computer by the NIT and sent to the FBI was accurately stored and reproduced. Tsyrklevich Declaration ¶ 6 (third bullet point). The defense does not need access to government servers to do this, however, because the government has agreed to provide an alternative method of verifying that the information obtained from Michaud's computer was accurately recorded. Specifically, the government has offered to provide a copy of the data stream sent by Michaud's computer to the government as a result of the execution of the NIT. Tsyrklevich can compare the information sent to the government by the NIT to the information provided in discovery to verify that what the government recorded from Michaud's computer is in fact what was sent by Michaud's computer. I have reviewed that data stream and, as explained below, confirmed that the information sent by Michaud's computer as a result of the NIT matches the information that is stored on the government's servers.

12. When two computers communicate via the Internet, they do so using standard network protocols. Communications over the Internet are sent in "packets," which serve as the means by which computers share information over a network. Just as two people communicating over email exchange individual messages, computers

exchange network packets. These packet exchanges follow standard network protocols that permit individual computers to process and exchange information with one another. Just like two people meeting on the street, computers wishing to communicate with one another first exchange greetings through a "handshake," then exchange information, and part ways with a communication exchange that basically consists of the computers saying "goodbye" to each other.[1]

13. Here, when the NIT was delivered to Michaud's computer, it had exactly this sort of interaction with a government-controlled computer. The network packets memorializing this exchange, which have been preserved in a standard file format, make it possible to reconstruct that exchange and see exactly what information was transmitted by Michaud's computer to the government.

14. A review of the data file, known as a PCAP file, documenting the exchange contains nine network packets exchanged between Michaud's computer and the government computer. Packets 1-3 correspond to the initial "handshake" that established the connection between Michaud's computer and the government computer. Similarly packets 5-9 correspond to the "goodbye" communication between the two computers. Packet 4 thus contains the substance of the communication—namely, the information collected by the NIT after it was delivered to Michaud's computer.

15. Reviewing this packet, I was able to confirm that the information collected from Michaud's computer matches the information stored on the government servers that has been provided in discovery. Each of the pieces of information the government-controlled computer recorded being collected from Michaud's computer by the NIT appears in Packet 4. If Tsyrklevich's goal is to verify the accuracy of the information stored by the government, then a review of the network data is all that would be required.

---

[1] Some protocols that are used to communicate via the Internet do not include a "handshake" as described in this declaration. These other protocols are not relevant to the matter at hand as the communications that occurred as a result of the deployment of the NIT did utilize a network protocol that included a "handshake".

EXECUTED: March 28, 2016.

DANIEL ALFIN
Special Agent, FBI