

The Honorable Robert J. Bryan

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

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

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

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

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

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

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

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

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

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

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

20 **B. The unique identifiers were in fact unique.**

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

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

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

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

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

11 11. Tsyklevich claims that he needs access to the server component in order to
12 confirm that the information obtained from Michaud's computer by the NIT and sent to
13 the FBI was accurately stored and reproduced. Tsyklevich Declaration ¶ 6 (third bullet
14 point). The defense does not need access to government servers to do this, however,
15 because the government has agreed to provide an alternative method of verifying that the
16 information obtained from Michaud's computer was accurately recorded.

17 Specifically, the government has offered to provide a copy of the data stream sent by
18 Michaud's computer to the government as a result of the execution of the NIT.

19 Tsyklevich can compare the information sent to the government by the NIT to the
20 information provided in discovery to verify that what the government recorded from
21 Michaud's computer is in fact what was sent by Michaud's computer. I have reviewed
22 that data stream and, as explained below, confirmed that the information sent by
23 Michaud's computer as a result of the NIT matches the information that is stored on the
24 government's servers.

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

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

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

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

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

25
26
27
28 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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28