EXHIBIT B

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**

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. 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. As an FBI Special Agent, I have been, on a number of occasions, tasked with the process of examining digital devices to determine whether

malware[1] was present on those devices and if so, to identify and analyze that malware. The purpose of such analysis is to determine the impact that the malware may have had on the device on which it resides or other devices with which the "infected" machine may have communicated. I have conducted this malware identification and analysis in both criminal and national security matters.

2. In each instance when I have been tasked with identifying and analyzing malware, I did not have advance knowledge of the specific malware for which I was looking or even if malware was actually present, though there was reason to suspect the presence of malware. I have nonetheless been able to locate, identify, and analyze suspected malware notwithstanding the lack of advance knowledge about the particular malware. In this declaration, I will lay out in general terms some of the steps that can be taken to identify and analyze malware and provide additional detail concerning the operation of the NIT used in the FBI investigation at issue in *United States v. Michaud*.

3. As a threshold matter, I would note that I do not consider the NIT used by the FBI to be "malware," though the experts retained by Mr. Michaud describe the NIT in such terms. The word malware is an amalgamation of the words "malicious" and "software". The NIT utilized in this investigation was court-authorized and made no changes to the security settings of the target computers to which it was deployed. As such, I do not believe it is appropriate to describe its operation as "malicious."

4. Prior to analyzing a device for traces of a malware infection and even without knowledge of the specific type of malware involved, an investigator generally has some information or indication of the presence of malware. For example, an individual's computer could be experiencing problems with programs failing to operate as intended or a user may notice that data have inexplicably been deleted from the

[1] The term "malware" generally refers to computer software that impairs the integrity or availability of data, a program, a system, or information. Other common terms that describe various types of malware are "virus", "trojan", and "worm".

system. Malware may also be responsible for sending data across a network or across the internet.

5. If malware does in fact transmit data over the Internet in a similar fashion to how the NIT transmitted data to an FBI controlled computer server, having a copy of the transmitted network data would be a valuable tool that would assist with analyzing a system and searching for malware. If the network data is not encrypted, it will generally contain strings of plain text containing identifiers that can be used as search terms during the course of a forensic analysis. Although the defense has declined to review the network data available in this case, I have reviewed and analyzed that network data. My review confirmed that it is not encrypted and contains various strings that would generally be considered valuable during the course of forensic analysis. For example, a defense expert who suspects that a given device was a target of the NIT could use these search terms to try and assess whether there are any traces of the NIT still left on the target device or if the NIT otherwise remains on the device.

6. Utilization of search terms is just one avenue of analysis available to locate and identify malware on a device. It is also possible to review the list of programs designated to run when a device's operating system loads. Such a review is a crucial step in determining whether a computer may be infected with malware. After identifying and eliminating from consideration known programs that the user intended to execute upon startup, an investigator may focus on any remaining programs whose purpose is unknown. In some instances, malware can be disguised as a legitimate program and can be identified by comparison of the legitimate program's file hash value against the hash value of the suspect program.

7. Where there is reason to suspect a storage device such as a USB drive or even a cellular telephone has been infected with malware, an investigator can undertake a dynamic analysis of any suspect files on that device and verify that those files either do or do not have the ability to execute malicious code. The process of conducting a dynamic malware analysis generally involves creating a copy of a suspect file and executing it in a

test environment. The state of the test environment is recorded prior to execution of the file and various programs are active in the test environment that record changes to the system. Additionally, various pieces of software or hardware can be utilized to capture any network data generated by the file upon execution.

8. I have personally executed the NIT on a computer under my control and observed that it did not make any changes to the security settings on my computer or otherwise render it more vulnerable to intrusion than it already was. Additionally, it did not "infect" my computer or leave any residual malware on my computer.

9. The devices seized from Mr. Michaud are available to the defense for inspection and review, and I believe, based on my training and experience, that the procedures describe above (among others) could be applied to those devices to determine whether there is evidence suggesting that the NIT or a piece of malware was responsible for the collection of child pornography found on Mr. Michaud's devices.

EXECUTED: May 19, 2016.

DANIEL ALFIN
Special Agent, FBI