EXHIBIT C

JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

UNITED STATES OF AMERICA, Plaintiff, v. JAY MICHAUD, *Defendant.*	No. CR15-5351RJB DECLARATION OF SHAWN KASAL

I, Shawn Kasal, declare under penalty of perjury that:

1. I am a network security consultant and a copy of my curriculum vitae is attached to this declaration. My professional qualifications include certifications and training from: Cisco, Microsoft, Apple/Mac, Novell/SuSe, Dell, HP, Oracle/Solaris, VMware, Red Hat, and IBM/Lenovo.

2. I have worked as a network and systems engineer for businesses over the past 15 years. During my employment for these companies, I have been responsible for investigating all forms of electronic fraud and network abuse. I specialize in e-discovery, data forensics, and network threat attrition/attribution. I have received electronic forensic education from a variety of sources, both from former law-enforcement/governmental agencies and private civil training. I have also contracted with General Motors, Ford Motor Company, and Daimler Benz to develop nation-wide network infrastructure security policies. In addition, I have worked for several ISP's (internet service providers), where I was responsible for shutting down "botnets," DDoS attacks (distributed denial of service), and other infrastructure hazards, including those that originate from the Tor network and P2P file sharing protocols.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

3. I have also served as an appointed and privately retained forensic expert on three federal cases involving the use of the FBI's NIT toolsets and methodologies. Among those cases, I worked in 2013 and 2014 with Dr. Matt Miller and Dr. Ashley Podhradsky in the collection and analysis of code necessary to audit the deployment of the NIT in *U.S. v. Cottom,* a case in Nebraska Federal District Court (CR13-108). The *Cottom* case arose from the FBI's use of an NIT as part of "Operation Torpedo," a Tor network child pornography investigation very similar to the one that led to the charges in this case.

4. I am currently retained by the Federal Public Defender office in Tacoma, Washington, to assist with forensic issues in the prosecution of Jay Michaud. In connection with this case, I have reviewed the various pleadings that have been submitted to the Court in connection with its NIT discovery order, including the declarations of FBI Special Agent Daniel Alfin.

5. As more law enforcement agencies face the challenge of investigating criminal behavior on "the Dark Net," the challenges also grow greater for the defendants charged in these cases and the courts that are called upon to understand and rule on often complex technical issues. "Network threat attribution" in the context of criminal investigations is a particular challenge.

6. "Threat attribution" means that a trial court and juries must assess whether the government's investigation techniques involved accessing data in ways that left a defendant's "network" (which may consist simply of a computer and any storage devices that were connected to it) vulnerable to errors attributable to the government's technique. In this case, was the targeted computer vulnerable to receiving illegal content from the government's own child pornography site along with or after the initial NIT breach? Or more likely (because third party malware, viruses and remote attacks have advanced faster than law enforcement can keep up) did the government's NIT leave the target computer vulnerable to separate attacks and viruses?

7. Such attacks, often involving the transmission, storage and distribution of child pornography in particular, are well documented. The illicit Internet child

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

pornography industry and distribution networks are massive, and some of the most sophisticated efforts to remotely transmit and secretly store illegal content on the computers of unwitting Internet users (including corporations and large networks) have been developed by pornography distributors. I have even worked on a Nebraska state court case where the defendant's cell phone was infected with a virus that routed child pornography through and to that phone. The virus was responsible for the transmission and downloading of child pornography to the user's phone, without his consent or knowledge. It was not until exhaustive analysis was done by the Nebraska State Patrol that we discovered the extent of the infection and determined that the defendant was not responsible for the offending material on the phone.

8. The FBI's use of an NIT in this case is cause for particular concern because the Government has offered no assurances (let alone evidence) that the multiple NIT components it deployed were properly audited and are consistent with the network security industry standards that are the bench mark for determining (a) whether NIT-type malware can be used without fatally compromising the security of the targeted computer system; (b) whether the NIT is designed to perform only those functions that were disclosed to the court that authorized its use; and (c) whether the data collected through use of the NIT is accurate and reliable.

9. More specifically, the National Institute of Standards and Technology (see nist.gov) maintains a list of approved, exhaustively tested, and stringent applications and standards that are key to determining the functionality and reliability of the type of digital forensic tools and technology at issue in this case. To my knowledge, the FBI has not provided any information to the Court about the testing and auditing of its NIT and whether it meets NIST standards. The FBI's apparent decision not to comply with the Court's discovery order is also preventing the defense from independently verifying that these standards have been met.

10. As a result of the FBI's response to the discovery order, there are now multiple technical issues that should be addressed to ensure that Mr. Michaud has a fair trial. Most broadly, judges and juries face a very difficult task assessing the

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

admissibility and reliability of evidence obtained pursuant to government hacking. The hacking tools and payloads of government malware are at the outset so obscured by technical problems and jargon that it is difficult or impossible for juries to assess the evidence and potential defenses without fully informed analysis and testimony from experts on *both* sides of the case. In this case, it appears that the government is relying on declarations from a case agent with little or no specialized expertise in forensic and code analysis, and at the same time trying to block the defense from using a team of its own experts to independently review and challenge the prosecution's claims.

11. The *Cottom* case, which also involved an FBI NIT, provides a helpful comparison. In *Cottom*, the government agreed to cooperate with the defense's discovery requests. However, the FBI later reported to the Nebraska court that it had lost part of the NIT source code. Given the potential harms and security issues the government has raised in connection with the disclosure of NIT information, the FBI's loss of NIT code in *Cottom* is still hard to understand. But there at least the government did not dispute the defense's need to analyze all of the available components and code to prepare pre-trial motions, a *Daubert* challenge, and potential trial defenses.

12. In this case, it appears that the FBI still has all of the discovery that the Court has ordered it to share, and that the Government has previously submitted a proposed protective order for that discovery. However, the FBI has apparently reversed its earlier position about secure sharing of this essential data. To my knowledge, the government has not provided an explanation for why the NIT discovery would be relevant and discoverable in *Cottom* and the other Operation Torpedo cases, but is not equally relevant and discoverable in this case. This is especially true since Mr. Michaud's defense counsel has informed me that he has offered to adopt additional security procedures for analysis of the code discovery that go far beyond anything discussed or considered in the *Cottom* case. In my opinion as a digital security consultant, the additional measures that have been proposed by the defense are quite adequate to ensure the security and continuing confidentiality of the discovery.

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Dated this 9th day of May, 2016.

Shawn Kasal

FEDERAL PUBLIC DEFENDER
1331 Broadway, Suite 400
Tacoma, WA 98402
(253) 593-6710

Shawn Kasal
Digital Forensic Expert
Consulting Engineer – Network Security Consultant
Omaha, Nebraska

Professional Experience

- Systems Engineer 15 years
- Privately retained to investigate all forms of electronic fraud and network abuse
- Specialize in e-discovery, data forensics
- Federal Expert Witness (Digital Forensics)
- CJA Expert Panel Federal Public Defenders Office
- Subject Matter Expert Network Threat Attrition/Attribution

Business and Organizations served

- General Motors
- Ford Motor Corporation
- Daimler Benz
- Sid Dillon Chevrolet GMC Cadillac Mazda Buick Hyundai Nissan
- Dillon Brother's Harley-Davidson
- Plaza Buick GMC
- Woodhouse Auto Group
- Wicks Truck Trailers
- Consulted with Infraguard and Cybercop
- Various local Banks and Credit Union's
- Various local Medical Practices and Hospitals
- Several law firms (NE, IA, NY, SD, OK, and KS)
- Federal Public Defender office (Omaha, NE) (Des Moines, IA)

Training along with Current and Previously earned Certifications and Certificates

- CompTIA A+ Linux+ Network+ Security+ Server+
- Microsoft MCP NT 4 MCSE 00,03,08,12r2
- Cisco CCNA, CCDA, CCNP with Wireless Networking, Routing, VPN specializations
- Data recovery in SANS NAS DAS environments
- Network attribution on Darknets (tor) (p2p) (other network obfuscation methods)
- CEH (Certified Ethical Hacker) training Version 8 courseware
- Compliance and Security Auditing PCI, HIPAA.

Software and Digital Forensics Training

- Linux, Windows, Mac OS, Mac los, Unix, BSD, Solaris, Android and related embedded platforms
- SANS Training, DOD Training, Former and Retired Law Enforcement
- Cellebrite cell phone forensic UFED (capture hardware)
- MOBLedit forensic capture methodology
- AccessData Group for Forensic Toolkit (FTK), ArcSight for ArchSight Logger. (syslog)
- Guidance Software for EnCase Forensics suite
- Paraben (P2 commander and i-recovery stick)
- Autopsy, open source graphical interface to The Sleuth Kit and other digital forensics tools.
- OS Forensic Suite, SANS SIFT
- BlackBag BlackLight Mac OS Forensic toolkit,
- White Glove Linux by Dr. Fred Cohen
- NIST forensic tools standards and qualifications
- Industry standard PC/Server/Laptop/Cellphone/Tablet capture and reporting software open or closed source
- E-Discovery/Network Intelligence software titles Splunk, Maltego, Alienvault, and Sentinel Visualizer