Robert M. Herz
Law Offices of Robert Herz, P.C.
431 W.7th Avenue, Suite 107
Anchorage, Alaska 99501
907-277-7171 Phone
907-277-0281 Fax

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

United States of America, Plaintiff, vs. Matthew Schwier, Defendant.	)	Case No. 3:17-cr-0095 SLG-DMS

SUPPLEMENTAL DECLARATION OF JEFFREY M. FISCHBACH IN SUPPORT OF DEFENDANT'S MOTION FOR PARTIAL RECONSIDERATION AT DOC.256

I, Jeffrey M. Fischbach, declare as follows:

1. In its most recent motion at Doc. 255, the government continues to attempt to impose its self-serving protocols on the defense. This motion, in one stroke, serves to limit the defense to *only* being able to conduct Mr. Erdely's own "validation", and prevents the defense from completing its own tests, which the court has already ruled are material. The government's sole assertion justifying its purported need for Wireshark is to prevent the accidental copying or distribution of its TD software. Implementing the use of WireShark does *nothing* to *actually* prevent the accidental or intentional distribution of its proprietary software. I would also note that, here again, the government makes no effort to even feign concern for potential harm to children -- commensurate with the charges. As such, the government continues to allow me unfettered access to

alleged child pornography *faciliated* by AUSA Jonas Walker, without so much as a protective order, while he continues to urge the court to impose arbitrary limitations on my ability to conduct tests, which even Walker himself, admits *do not* actually serve to prevent its software from "escaping into the wild".

2. Specifically, I agree that Wireshark is a very useful tool to observe any nefarious *or* legitimate use of any computer computer IO (input-output) port, including wireless. Since I agree to this premise, it would seem the government's need to call a witness is unnecessary just to testify to this fact. The government makes no assertion that Wireshark does *anything* to prevent the copying of its software. The fact is that it does not. Its only function is to record the transmission and receipt of data on the host device. According to Wireshark's own website: *"What is Wireshark? Wireshark® is a network protocol analyzer. It lets you capture and interactively browse the traffic running on a computer network."* (https://www.wireshark.org/faq.html#_what_is_wireshark). I agree that Wireshark -- if configured to do so, and if started, and if it is left uninterrupted, *by me* -- will record the [accidental] copying of TD. But only if all those things happen, and only if *I* allow that action to be recorded. What it will also record is *every single element of my testing*, as data is transmitted for testing purposes, moment-by-moment, in exhaustive detail. And the only way Mr. Walker will have the ability to even make the accusation that TD has been "released to the wild", intentionally or accidentally, will be for him, or more likely, someone working for him, to decrypt and analyze my detailed recorded work product -- if so ordered by the court. And in doing so the government will have accessed attorney-client privileged data and obtained protected attorney work product information.

3. I am arguably one of the best equipped people on the planet to steal this software without anyone ever being the wiser. And I can do it *while* Wireshark is running. Now after questioning my credentials for almost two hours on the stand, Mr. Walker has pivoted to his "concern" that I might "accidentally" copy the

software. Perhaps Mr. Walker is prone to accidentally copying or deleting files on his own computer, but I have been working with sensitive files for a quarter-century. Many of the procedures used by the FBI today were first used and instructed by *me.* So long as I have complete and unfettered access to properly determine and configure the equipment I use for these tests, I will take all the agressive file containment protocols that I *always* use when examining sensitive material. This however, will necessarily require me to configure all equipment myself, and have access to add and remove all necessary software as my time-tested and industry-accepted protocols dictate, which means I will need access to more than one port on the government provided computer. If I am allowed to do this I can safely guarantee the TD software will not be accidentally copied or distributed while under my control. Should I be required to use the computer as dictated by the government, without the ability to install or connect any previously tested and industry accepted software (much of which is specifically designed to protect data from any unintended use) or hardware to *any* port or connector on the computer, as needed, then not only can I not complete my tests, I would not be able to assure the court that all standard precautions had been taken.

4. Mr. Walker brings to the court's attention the theft of a hard drive I left in the *government's* custody, care, and control. In what can only be referred to as an opportunistic loose association with truth, Mr. Walker makes the unsubstantiated and false claim that "Mr. Fischbach has, already, *lost* a hard drive at the OCRCFL in this case." Mr. Walker is well aware, via his intrusive interrogation of my assigned RCFL liaison, Joseph Monroe, that Mr. Monroe did not describe my hard drive as being "lost". He described it as "missing" from the Defense Review room, where I am *required* to keep it, in order to allow me to continue processing data overnight or over the course of several days. Which, in order to complete my work for trial, without delay, is both necessary, and facilitated by the RCFL. Mr. Monroe has documented by email, dated July 2, 2019, his knowledge that the

processing (long periods of time the computer works without examiner input) of my examinations were ongoing, in my absence. He specifically requested my permission to allow someone to disconnect the equipment, in order for another examiner to use some of it. In an email from Mr. Monroe, solicited by Mr. Walker, documenting his observation of my examination, Mr. Monroe wrote the following: *"Only Fischbach and Herz came back on 25th. Fischbach advised he was missing an external hard drive that he left in the Defense Review room, during his last visit. We were unable to locate the missing external hard drive."* As Mr. Monroe was aware, that drive was connected to the *government's* work station -- as it was when the work-station was in Anchorage, supervised by Kyle Reardon.

5. Despite my request to use two *significantly more* secure private exam sites -- FBI Wilshire, and Roybal Federal Court's SCIF, both of which I have successfully used many times without incident, and both of which are *significantly* shorter drives for me -- it is Mr. Walker who has insisted that I use the OCRCFL, where he is, apparently, able to maintain a closer watch on my work, and with whom I work. Mr. Walker should know, however, that unlike the FBI and LA SCIF, the OCRCFL offers *only* a shared work space where many different civilians and RCFL personnel come and go and even share much of the same equipment. I would agree that the OCRCFL is a location that *does* risk the possible theft, not only of TD, but of the *entire computer* upon which it is installed. Frankly I am surprised, given the government's purported concern about the security of its TD software that it has not readily accepted my offer for the defense testing to occur in the federal court SCIF. Not only can the OCRCFL not guarantee that items will not be stolen from its own Defense Exam room, it apparently does not take seriously its role in protecting details concerning the use of its defense work environment from the government. What Mr. Walker does not know from his heretofore unjustified intrusion into my RCFL work is whether the

missing drive, taken from the RCFL Defense Review room, when I was not present, was encrypted to secure its contents so that only I could personally decrypt them, or whether that encryption was set to wipe the drive upon unauthorized attempts to open it, or whether the drive had tracking measures installed, or whether that drive has since been found and returned to me thanks to any of the above measures. While Mr. Walker does not have an explanation for how Wireshark *in any way* prevents the theft or accidental copying of its software, (which it emphatically does not,) I can assure that court, given unfettered access to *all* testing equipment, that I *will* guarantee that, in my hands, the software will not escape the OCRCFL. I cannot, however, make the same guarantee for the TD copy the court's order requires be left with FBI or OCRCFL personnel.

6. Much like Mr. Walker knew that Internet access was *required* to test Torrential Downpour, he also knows that it was the RCFL that "lost" a hard drive left in *their* care. He also knows that in order for Wireshark to be used in the way he proposes, I would have to be *trusted,* unmonitored, by myself, to actually configure it the way he wants me to, and to use it, without interruption or log file alteration, to record *all* of my activity on the computer the government will provide. Moreover, like the TD secrets already accidentally exposed to me, and the missing hard drive I reported to the OCRCFL, the only way that the government would even know that their software escaped the RCFL lab is either if *I* can be trusted to report it to them, or if they actually plan on arbitrarily demanding the examination of the Wireshark recording they trusted *me* to make. By which time, given their self-imposed requirements, the software would be irretrievably lost to "the wild". On the other hand, examination of these Wireshark logs by the government would give them a very complete reenactment of my tests; tests protected by attorney-client privilege and attorney work product doctrine.

7. As noted by the government, the court ordered, "On or before Monday,

November 25, 2019, the government will provide the defense with all applicable TD software documentation for versions 1.15 and 1.23, including installation instructions and minimum operating requirements." And that, "Not later than Wednesday, November 27, 2019, the defense shall provide to the government the specifications for the computer that it is seeking for TD testing." The court clearly understands my limited ability to determine appropriate specifications for the hardware and equipment I need to test the software, without first being provided any documentation or specifications relating to the software to be tested. In its motion at Dkt. 255 the government has instead chosen to ignore the court's order to provide complete documentation and equipment specifications, and ignores, as well, the equipment specifications I already provided without the benefit of the materials now ordered by the court. Mr. Walker instead has seemingly made the arbitrary decision to provide a piece of used equipment, similar to the vintage equipment it has already provided to the OCRCFL without any reference to the specifications provided to him by the defense already. Mr. Walker has nowhere in Dkt. 255 explained why the court's order to provide TD documentation and equipment specifications is unreasonable or untenable. He simply seems to believe that his judgment of what I need to complete my tests supersedes either the court's or mine.

8. As such, the government has <u>not provided installation instructions or minimum operating requirements</u>, (per my previous requests, or the court's order), with its heavily redacted TD User Manual for version 1.23. At Mr. Walkers request (November 19, 2019 email), the following equipment estimates were provided: Apple Macbook Pro Laptop, 2.8GHz quad-core Intel Core i7

processor, 64GB memory,, 512GB SSD storage, Thunderbolt / USB-C, WiFi/RJ45. (Updated and summarized here.) While outwardly similar to the equipment Det. Erdely used to perform his "validations", this equipment was specifically chosen, with the expectation that, while accommodating the operating system and software I was able to *observe* Erdely using for his "validations", it should also provide an environment that will accommodate the forensic hardware and software I need to install in order to both complete my testing and assure the court that the machine has in no way been compromised during my testing, and that no software or data has been lost, stolen, or compromised. This hardware has some other very specific capabilities which are routinely utilized by forensic technologists, that are both necessary to complete my tests in time for trial, as well as to secure the equipment, software, and data from theft, intercept or alteration. While it is my usual practice to consult software specifications before choosing hardware, in the absence of court-ordered specifications, *this* hardware is suited to accommodate my anticipated needs for TD testing, as described previously to the court, while allowing me to use industry-standard practices to protect the software, data, and equipment. The equipment Mr. Walker has described in Dkt. 255, is not.

9. The court's order for documentation materials, quoted above, is in no way ambiguous or silent to its documentary requests, nor does it speak to any redactions. Mr. Walker previously claimed, while on record, that no such documents exist, but now he says they need to be redacted. Similarly, after affirming to the court that software change logs did not exist, they suddenly do.

10. The court order to "provide the defense with all applicable TD software documentation for versions 1.15 and 1.23, including installation instructions and

minimum operating requirements," is clear and unambiguous. However, as he has done previously in this case, Mr.Walker is again opportunistically interpreting the court's lack of granular specificity to mean "redacted" material, as the government sees fit to define "privileged information". Again, I remind the court that Mr. Erdely stated under oath that TD's secret identity was it's *only* secret. Yet the government continues to claim that there are other things which the defense should not be able to see. One of those things may be responsible for the reason that TD investigations across the nation have, on several occasions, been inconsistent with the findings of well-tested, industry accepted software and hardware. As is the case herein.

11. Given the necessary access I need to complete my testing on the equipment provided by the government, I will take all necessary software and hardware precautions to restrict copy or dissemination of TD, and to secure my forensic work environment, as has been my standard practice for 25 years.

12. The foregoing statements are true and correct to the best of my knowledge, and I hereby reserve the right to amend them should additional information be made available to me at a later date.

/ / /

/ / /

/ / /

I declare under penalty of perjury under the laws of the United States and the State of California that the foregoing is true and correct, and that I execute this Declaration in Los Angeles, California, on November 25, 2019.

Jeffrey M. Fischbach