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

DECLARATION OF JEFFREY M. FISCHBACH
IN SUPPORT OF DEFENSE MOTION FOR RECONSIDERATION

I, Jeffrey M. Fischbach, declare as follows:

1. In its "ORDER RE MOTION FOR ADDITIONAL TERMS FOR PROTECTIVE ORDER (Dkt. 254)" the court has demonstrated clear efforts to strike a balance between the need for the defense to complete tests which the court has found to be material, with the government's concerns regarding *potential* distribution of its proprietary software. However some government language adopted by the court, makes it impossible for me to conduct the tests which the court has found are material to the defense. Mr. Walker himself, has admitted that the arbitrary limits he has asked the court to adopt, *do not* actually serve to prevent the government's software from "escaping into the wild". Specifically, the government's arbitrary constraints on how I physically can and cannot access the government's own equipment prevents me from conducting the defense tests that I must complete for trial. I do believe, however, that this may be a simple misunderstanding of the software and equipment necessary

to complete testing and subsequent analysis.

2. Without unfettered access to computer ports, in order to install my own tested, industry-accepted software and hardware, as well as to remove my test results from the government provided computer for further examination and analysis at my laboratory, I simply can't complete the tests that the court has found material to this matter. With current restrictions in place, I can't even connect a screen, keyboard, or mouse, let alone the hardware and software that I need for my tests, and that are required by industry standard forensic practice in order to insure that no data accidentally alter my results or escape the system. As Agent Allison should well know, some of the most effective industry-tested forensic standard software *requires* a USB dongle (key) to remain plugged into the computer's USB port, in order to use the software. Indeed, this USB key was necessary and *required* for Allison to use the software he relied upon in his own work to forensically examine the evidence seized from Mr. Schwier's property. The very same software that produced results inconsistent with TD. Thus, had Agent Allison been subject to Mr. Walker's restrictions of only connecting to one network card port, even he could not have completed his own exam which alerted the defense of these inconsistent findings.

3. If Mr. Walker isn't aware that his arbitrary restrictions limit my work to only reproducing Mr. Erdely's "validation" procedures, then he simply hasn't done his homework or consulted with his own experts. This not only restricts me only to performing Mr. Erdely's "validation" procedures, but it doesn't even allow me to competently utilize the tools available to me to personally assure that no unintended data enters or exits the machine, as Mr. Walker himself claims to fear. I see no scientific or investigative value to utilizing precious resources repeating Mr. Erdely's "validation" here in California. On the contrary, I refuse to be associated with the propagation of "junk science", as dictated by an apparently biased actor, who clearly doesn't understand scientific method or computer security.

4. To a significant degree, the court relied on the government's [PROPOSED] ORDER GRANTING MOTION FOR ADDITIONAL TERMS FOR PROTECTIVE ORDER filed on

November 18, 2019, which was little more than a superficial makeover of their prior proposal which *only* served to allow me to perform ***their*** proposed "validation", and not my tests. It appears to me that the court was able to recognize that tests conducted under the government's own prescribed "validation" procedures would effectively neutralize decades-old practices of independent review. The court's current order seems to address *most* of those arbitrary government constraints.

5. In order to clearly articulate for the record why I am unable to effectively prepare counsel for trial with certain remaining restrictions, I will address my remaining concerns within Dkt. 254 line-by-line in the following paragraphs. Paragraph numbers in **bold** reference and correspond to the numbered paragraphs in the court's order at Doc.254.

a. ***(Paragraph 6)*** *Government personnel will have access to the TD Computer only for the purposes of starting the TD Computer, entering the password for the defense, and keeping the TD computer secure consistently with OCRFCL standard operating procedures. Government personnel will not observe the defense testing.*

Rather than relying on AUSA Walker's self-serving interpretation of OCRCFL standard operating procedures, I would urge the court to compel Mr. Walker to produce text from the actual SOP upon which he claims to be relying. Based on his insertion of government personnel into a defense examination, I don't believe he has even consulted the RCFL. I have personally utilized several RCFL facilities around the country. Contrary to Mr. Walker's representation, it has been my experience that RCFL personnel have been instructed specifically *not* to interact with equipment used by the defense, specifically because doing so risks physically observing privileged work product, and can lead to accusations of government "snooping".

In this particular case, Mr. Walker has *already* asked the OCRCFL's Joseph

Monroe to provide details about my examination. Should Mr. Monroe, (or other RCFL staff) be in control and custody of the equipment containing my work product, they would be able to see my examination progress each time they have to log me back into the system (which happens every time I so much as leave to use a restroom), as well as hold exclusive possession of the password to access it while I am away, he (they) would most certainly be suspect, should my tests or the computer fail, or should the government appear to gain advanced knowledge of my testing results. While this may not have previously been as great a concern when Mr. Reardon was assigned to the case, it has been of particular concern given Mr. Walkers already proven proclivity to use RCFL staff, with no apparent justification, to provide information about my examination, communication, and consultation. While I do understand that the AUSA does have the power to use the RCFL in this way, I seriously doubt that it is the court's intention for him to continue do so.

Any government access to my tests and/or testing environment (hardware/software), including set-up, risks attorney-client privilege and work product, my ability to authenticate my own work, inserts the government into the defense chain-of-custody, and could invalidate my test results. A technically knowledgeable Agent can learn a lot simply from the hardware configuration and setup and the software I am using to perform the tests I need to conduct. The government has not justified how being granted sole password access to my tests, and physically opening the screen every time I need to use the computer, *in any way* serves to secure its software or equipment, (or serves to protect children,) when the equipment itself will already be in the *physical* custody of the government to begin with. Despite his knowledge of the stolen hard drive I reported to Mr. Monroe, Mr. Walker does not so much as specify any need or requirement for well-established forensic software/hardware measures that could be used to *actually* protect the equipment and data (including TD software) against being physically stolen or accessed from the RCFL.

With the physical restrictions pertaining to access to the government computer, noted below in Paragraph 9 of the court's order, which were imposed at the government's request, I can't even install and utilize these standard measures, let alone the software/equipment I need to perform my tests. All of which leads me to believe that either Mr. Walker is simply naive and has not done his homework, or that his real motivation is to thwart my examination of TD software and/or use it to prove that I have in some way violated a court order, so that he can either eliminate or damage my testimony in the defendant's case.

Moreover, in *no way* is *any* of this "consistent with OCRCLF standard operating procedures". This is blatant misrepresentation to the court. Mr. Walker himself provided me the password to the computer currently housed at the OCRCFL. Mr. Monroe, to my knowledge has had *no* access to this password or even touched the keyboard of that machine. This does, however, further justify the need for me to have complete, unfettered control over my equipment, including exclusive password control, not shared with the government, while conducting tests at the OCRCFL

> b. ***(Paragraph 7)*** *Installation of Torrential Downpour software onto the TD Computer will occur as follows:*
>
> > i. ***a.*** *An FBI agent or Task Force Officer will keep exclusive possession of a USB drive or other removable media containing the Torrential Downpour software. The defense will not possess the Torrential Downpour software, other than on the TD Computer.*

I have consistently agreed that the RCFL should maintain custody of the TD installation disk provided to it. As Mr. Monroe himself has conceded, my own equipment which I was required to leave at the OCRCFL, was stolen from the OCRCFL's Defense Exam room, while I was not present, and while in the custody and control of the government. It would certainly be prudent to make sure that this software is kept secure. However, the tests that were ruled material *do* require testing and analysis of TD which *necessarily* requires that I

make multiple copies subjected to industry-tested software and hardware analysis. Therefore, while this can all occur within the confines of the OCRCFL, it simply cannot be completed, *in any way*, on a machine restricted in the way the government has outlined. Again, the government's proposed order simply allows for me to conduct Mr. Erdley's "validation" in California, without Det. Erdely's physical presence.

> ii. ***b.*** *Prior to testing, the FBI agent or Task Force Officer will allow Mr. Fischbach to install Torrential Downpour versions 1.15 and 1.23 onto the TD Computer, all while in the physical presence of the FBI agent or Task Force Officer. The FBI agent or Task Force Officer may observe Mr. Fischbach install the software.*

Mr. Walker has already reached-out to OCRCFL personnel to gain intelligence on my previous examinations and work. Since the passing of the Adam Walsh Act RCFL "Walsh Rooms" (Defense Exam rooms) have been treated as a "firewalled" environment where defense examiners can conduct their work without exposing privilege or work product. The government now seeks to breach this "firewall", which only serves to undermine operational practices that took years to establish. If the government's restrictions are upheld, it could undermine the trust and use of these facilities by defense examiners across the country.

Mr. Erdely's protocols included starting screen capture & monitoring software, as well as Wireshark, *before* the installation and initiation of his software. My time-tested industry-practiced methodology also requires the initiation of certain hardware and applications on each work-station prior to testing and examination, which would necessarily make the observing agent privy to attorney client privilege. At the same time, unless that agent or individual *is* well trained in computer forensics, it is unlikely that he/she would serve *any* value to the government in terms of securing its software. On the other hand, if this individual *is* technically-trained, then he/she serves an even greater value as an "information spy" for Mr. Walker, than in any way to actually secure software.

> ***c.*** *After the installation, the FBI agent or Task Force Officer will remove the USB drive or other removable hardware from the TD Computer.*

The government should continue its now long-standing practice of having a *hands-off* policy when it comes to defense forensic examinations. As I have continued to offer, I would encourage the safe custody of the original software in government hands, and I would be willing to personally put it *in* the government's hands the moment I have completed my use of the installation files. More significant in this paragraph, however, is the government's continued use of the term "TD Computer". This further emphasizes that the government intends for me to operate *exactly* as Mr. Erdely's "validation" protocols specify -- not according to my own testing protocols, that this court has already ruled are material to the preparation of the defense in this case. This notion of a "TD Computer" is simply because Mr. Erdely's protocols specify one computer as "TD", and the other as "Suspect". As outlined previously in my redacted declaration, that is not my proposed operating procedure. And that *will not* allow me to complete the tests that have been found to be material in this case.

> ***d.*** ***(Paragraph 8)*** *The defense may bring digital media, computers, cell phones, and an internet hotspot (i.e. one that is compatible to connect to the TD Computer via the network card) into the OCRCFL room with the TD Computer.*

Again, the government sees fit to dictate the defense examination environment, in order to restrict defense testing to its own "validation" protocols. In this case, however, the government is dictating an Internet connection method (Ethernet) that is currently unavailable on most Cellular 4G hotspots, and one that was not even an option on the WiFi hotspot that Mr. Erdely used for his own "validation". If a WiFI connection is unsuitable, or vulnerable, then it begs the question: why did Mr. Erdely use WiFi himself? I suspect that this government proposed requirement was made simply because it is well known that

there are very few "hotspots" for sale that have a wired Ethernet connection, and that those would be very costly for the defendant. For example, a simple search will show that the only Ethernet-equipped hotspot available from Verizon costs more than 4X as much as a comparable WiFi hotspot from Verizon. ($649.99, compared to $149.99.)

> ***e. (Paragraph 9)*** *The TD Computer will contain one network card. The defense will not make any connections to the TD Computer other than through the network card. The TD Computer may access the internet through the network card.*

As stated above, the government seeks to narrow the defense testing and examination to its own "validation" procedures. In order to complete the tests that have been deemed material, I simply *must* have the ability to connect my own equipment, install my own industry-tested and accepted software and hardware, and to have the ability to remove my results for further examination and analysis. Otherwise, I *cannot* complete the testing that has been found material in this matter. In short, I need access to multiple computer ports and network connections to run my tests.

> ***f. (Paragraph 13)*** *The defense will not tamper with or open the TD Computer.*

I understand and concur with the apparent *spirit* of this paragraph, I would for all of the reasons stated above, ask that the court impose the same admonition on the government. To that end, I had previously considered "tamperability" in my prior equipment specifications *estimate* that was provided to the government last week. Although a desktop machine is considered to be easier and less expensive to repair and upgrade, and has always remained my preferred platform for that reason, I would likely seek to use a laptop for my tests, because while retaining similar capabilities, they are significantly more difficult to alter, and much easier to identify any tampering that has occurred. For several reasons (which I can provide, if necessary, in a redacted document), including this, I tend to rely on Apple laptops, when an examination requires leaving equipment in government custody. At little-to-no added cost compared to similarly-

equipped desktop machines, I believe these safeguards serve to protect and authenticate chain-of-custody, work-product privilege, as well as *both parties* from any associated accusations.

6. 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 aggressive 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 and more than one network connection. 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) and 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. Given the necessary access I need on the testing 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.

7. The foregoing statements 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