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

I, Jeffrey M. Fischbach, declare as follows:

1. This declaration is written in response to the government's Dkt. 288, "Notice Regarding Proposed Testing Environment", and 288-1, "Test Environment Regarding Torrential Downpour".

2. In both writing my November 25, 2019 Declaration, and at the hearing on November 26, 2019, I attempted to articulate compromise, in order to assuage the government's concerns for its proprietary software; while remaining focused on the tests deemed necessary in order to competently prepare counsel for trial. At the same time, I have attempted to observe and

maintain sound scientific and forensic practices -- both necessary to survive a Daubert-Frye challenge, as well as to assure the integrity of my results and to ensure the security of my work product and of the software in question.

3. It appears that the government has almost wholly superseded its Dkt 253-4 with new, much more harsh restrictions proposed in Dkt 288 and 288-1. Nearly every item proposed in Dkt. 288 and 288-1 serves to add additional impediments to Torrential Downpour (TD) testing of any kind, adds several new means for the government to monitor and surveil defense testing, *in real-time*, exposing work product and privilege in the testing process. Yet, while this new proposal adds numerous barriers to performing the tests that the court found material, it does nothing to prevent TD from "escaping" into the "wild".

4. While the defense has objected to being forced to create discovery of its own testing procedures; in Dkt 288 and 288-1, the government has now gone much further than its proposal in Dkt 253-4. As an expert for decades, I understand that my results will be subject to scrutiny-- if used at trial. Hence, I understand I will have to document my work, as well as the forensic measures I have taken to protect assets, such that it could be independently reproduced. The means of doing so, however, has never been dictated to me by the government or by the court.

5. Confirmation bias has long plagued forensics. But, in this particular circumstance, the capability to narrow recorded results by using Wireshark's built-in filters was actually demonstrated by Mr. Erdely during his "validation" sessions. Thus, with the government documenting my work, not only do they see my test results before I can even report them to counsel, but I have no ability to audit my own discovery for accuracy. I testified on November 26, 2019 that Dkt 253-4's proposal that I must maintain a Wireshark log of all my work could be easily manipulated. As a result, it seems, the government has now proposed in Dkt 288-1 that *it* must be able to record and maintain easily-manipulated Wireshark logs of all of my testing, as well as control the router which carries all of my testing traffic. Which, in addition to *very* realistically altering my results before I read them, or for the government to collect conflicting results, it also gives the government the opportunity to filter, intercept and modify every piece test input data from one machine, before it even reaches the other, or to return

modified results. Submitting to this proposal has the making of a forensic science scandal rivaling any of the recent FBI lab scandals. Again, I refuse to be a party to bad scientific practices and dangerous precedent.

6. Dkt 288 and 288-1 does, however, carefully dictate the way that the defense can conduct its tests by not only providing an environment designed around Mr. Erdely's TD "validation", but then completely denying the defense use of the Internet for its testing. Something which Mr. Erdely himself stated, during his validation, was a *requirement* for using TD in any way.

7. Despite the government's failure to secure its own software and secrets, I have gone to great lengths, both to voluntarily alert the government and the court about information which they accidentally provided to me, as well as to attempt to use equipment owned by the government, at facilities run by the government, and to utilize very expensive specialized hardware and software at my disposal to further reduce the risk of accidental dissemination. To wit, I suggested the use of the LA SCIF, when it was demonstrated to me that the OCRCFL does not physically guarantee the security of equipment and data left in its shared defense exam room.

8. In Dkt 288, p7 the government refers to my suggestion to use the Roybal SCIF as "unusual" -- not untenable. All parties seem to agree that RCFL facilities are not equipped to monitor against theft of hardware and software, as has already occurred in this case. Out of an abundance of caution, based on decades of experience with government examination facilities, I have provided objectively more secure alternatives to the OCRCFL. In my experience, the SCIF in Los Angeles are simply isolated single rooms, containing no access to sensitive information, *other than that which the analyst is currently examining.* Thus, while this may be a "inconsistent" use-case, the treatment of software as "government sensitive" is also inconsistent with all standard investigative software, which have been openly tested and utilized by the forensic community. I have had access to the SCIF in Los Angeles, where I had permitted use of my own laptop and cellular devices, with only the admonishment of a "lifelong obligation to protect from disclosure the classified information" to which I had access.

9. The government refers to "*general"* principles of SCIF operation. Thus, one can assume

that these principles apply generally, but not exclusively. And, that while my suggestion for a more secure location to conduct my TD tests is "unusual", it apparently does not go against any particular rules or policies. It should be further noted that, in my *proven* classified experience, while information relative to a particular case is stored in a particular locked and secured SCIF room, the SCIF itself does not provide information to any classified or other case information, beyond the immediate case being examined.

10. I see no reason provided in Dkt 288 to explain why the LA SCIF cannot be used, nor why it is any less secure than the OCRCFL. While the government is correct that the LA SCIF at Roybal is several hours closer to me, which will allow me to complete my work significantly faster, security is the primary reason I suggested this facility, as well as the LA FBI building at Wilshire. I suggested both of these locations before the government decided to impose use of OCRCFL. I have used all three locations in Federal trials many times, and have been long aware that the RCFL does not provide security comparable to the other two sites. Thus, when requesting the ability to continue examining the case in Los Angeles in order to expedite trial readiness, I suggested either the LA Wilshire FBI defense examination facilities or the Roybal SCIF -- for the purposes of hardware, software and data security as well as location.

11. Dkt 288 and 288-1 provide conflicting information, by arguing *both* that I can't use the SCIF because I need to use the Internet and some of my own hardware to conduct my tests, *and* that I can no longer use the Internet *or* my own hardware at the RCFL. While Dkt 288-1, paragraph 3 proposes, "No other electronic devices or storage devices may be brought into the testing room to include but not limited to computers, phones, laptops, hard drives, or tablets", Dkt 288 (Page 8) states, "...the evidence review includes use of the internet and the presence of Mr. Fischbach's computers. Therefore, the SCIF is not an appropriate place for evidence review in this case." It appears here that the government acknowledges the need for the defense to utilize its own equipment and Internet service to complete its testing, for the purposes of denying use of the SCIF, yet denies defense use of its own equipment and Internet service for the purposes of using the less-secure defense examination room at the OCRCFL.

12. Similarly, while Dkt 253-4 (Para 6) specifies exactly what kind of Internet device I may

bring to conduct my tests, Dkt 288-1 (Para 5) completely denies *any* use of the Internet at all for testing. And, while Mr. Erdely has gone on-record that TD *requires* use of the Internet for the "validation" he performed in my presence on November 4, 2019, or use of any Torrent activity, the government has, in Dkt 288-1, once again proposed an environment that appears nearly identical to Mr. Erdely's "validation" methodology. Dkt 288-1 doesn't even allow me to conduct Mr. Erdely's own "validation" procedures, let alone the tests the court has already ruled material.

13. Preventing data from being disseminated is one of the key roles of the established forensic hardware I use in my testing and examination. In this new proposal, while the government suggests that its interests are in protecting the software that *they* have already accidentally released to me *without* any of their proposals in place -- I have now been completely restricted from using any equipment to secure any subsequent copies.

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 December ???, 2019.

Jeffrey M. Fischbach