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

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

United States of America,	)	
	)	
Plaintiff,	)	
	)	
vs.	)	Case No. 3:17-cr-00095 SLG
	)	
Matthew Schwier,	)	
	)	
Defendant.	)	

A period of excludable delay under 18 U.S.C. 3161(h)(1)(F) may occur as a result of the filing/granting/denying of this motion/pleading. As of the date of this filing 36 days remain before trial must commence pursuant to the Speedy Trial Act

MOTION FOR PARTIAL RECONSIDERATION OF THE COURT'S ORDER AT DOC.254 RE: ADDITIONAL TERMS FOR PROTECTIVE ORDER

Comes now, Matthew Schwier, by and through counsel, Robert M. Herz of the Law Offices of Robert Herz, P.C. pursuant to L.Civ.R. 7.3(h)(1)(A), and the fifth and six amendments of the United States Constitution, hereby moves this court for partial reconsideration of its Order at Doc.254 due to a "manifest error of fact."

On November 8, 2019 the court ordered the government at Doc. 243 to provide the defense with a copy of the government's secret proprietary software "Torrential Downpour" used by the government in its surreptitious investigation of Mr. Schwier in this case, so that it could be subjected to independent third party testing, to test among other things the reliability and accuracy of the software. The court gave the government 7 days to comply with the order. The court also invited the government to propose additional terms to the protective order previously entered at Doc.231 if "warranted." On the day the government was ordered to release the software, the government at Doc.244 filed a motion seeking to add terms to the protective order previously issued at Doc.231. Following additional briefing by the parties, the court issued the Order at Doc.

254 which added additional terms to the protective order at Doc. 231, and from which the defense now seeks partial reconsideration.

The most significant manifest error of fact in the court's order is paragraph 9 which limits the defense to the use of one port and network connection. Factually this error, as explained by Mr. Fischbach in his Declaration in Support of this motion filed herewith, will make it impossible for him to conduct any of the proposed defense tests which this court has deemed material to defense preparation for trial. See, Fischbach Declaration in Support of Defense Motion for Partial Reconsideration of Court's Order at Doc. 254 [hereinafter "Fischbach Declaration]. See, e.g. paragraph 2 and 5e.

As Mr. Fischbach notes: this restriction prevents him from installing industry accepted software and hardware as well as prevents him from removing his test results from the government provided computer for further examination and analysis on his own equipment, and/or in his own forensic work environment. He would be unable to connect a screen, keyboard, or mouse, let alone the hardware and software that he needs for his tests. The hardware and software required and vetted by industry standard forensic practice would insure more than any prophylactic proposed by the government that no data accidentally alter results or escape the system. Specifically, he writes:

> 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.*

See, Fischbach Declaration at paragraph 5(e) emphasis supplied. This factual error in the court's order must be corrected in order for defense testing to be accomplished.

The manifest error of fact in Paragraphs 6 and 7 of the court's order is that these additional terms compromise attorney-client privilege and attorney work product by intruding

upon the confidential and independent defense testing process. These restrictions do not actually provide security to prevent the loss of TD software "into the wild," but they do prevent the defense from conducting its tests properly and from implementing time-tested forensic-standard procedures (software and hardware) for securing sensitive data. See, Fischbach Declaration at 5(a)-(c). Moreover, requiring the government to be the sole possessor of the password protecting the TD test equipment, both inserts the government into the defense chain of custody and also makes it impossible for Mr. Fischbach to be held accountable for securing either the TD software or his own results as the government now has access to defense work product. Indeed, the only person who should have sole access to defense work product is Mr. Fischbach, and as such he should have sole and exclusive possession of any passwords. Mr. Fischbach sets out the problems presented by these restrictions in detail in his declaration but a few highlights appear below.

While having the government start the computer each time and enter a password seems innocuous, it is not. First it is not consistent with RCFL standard operating procedures (SOP), contrary to the government's assertion. RCFL's have a "hands off" policy regarding defense testing and equipment. Fischbach Declaration at paragraph 5(a) and 5(b) sub (c). If the government is in control and custody of the equipment containing defense work product, the government would be able to see the examination progress each time they log Mr. Fischbach back into the system. As Mr. Fischbach writes: "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." *Id*. at 5(a). Moreover, time-tested industry-practiced methodology 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. If this individual is technically-trained, then he/she can serve can as a conduit of privileged defense information to Mr. Walker. *Id*. at 5(b) sub (b). Mr. Walker has shown a proclivity for relying on information provided by observing Agents,

e.g. Mr. Monroe's recent email describing defense testing personnel in this case on September 25, or procuring a FBI-302 from the Agent observing the defense testing in the *Gonzales* case. The restrictions in paragraphs 6 and 7 of the court's order do not actually make it less likely that the TD software is inadvertently disseminated but they do seriously compromise the security of privileged defense information and data.

Lastly, in paragraph 8 of the court's order at Doc.254 the court limits the defense Internet connection to a single wired Ethernet connection. The factual error here is the assumption that TD software is less secure using a standard WiFi connection, and somehow more secure without the ability of Mr. Fischbach to install industry vetted forensic hardware and software. Were this true then Det. Erdely would have used a wired Ethernet connection himself when conducting his "validation;" but he did not. He used a standard WiFi connection. There is no valid basis to restricting the defense to a wired Ethernet connection which is substantially more expensive and is not available in many places.

Conclusion

The court has found the TD software is material to the defense and that the defense is entitled to conduct independent defense testing. This testing cannot be completed and is impossible without access to multiple ports and network cards. Allowing government Agents to access the computer at start up, perform log in and enter passwords not only affects testing reliability and validity but compromises sensitive and privileged defense data. Lastly, requiring a wired Ethernet connection offers no appreciable security but adds expense to the defense and may not even be available. Attached hereto is a defense proposed Order modifying those paragraphs in the court's order at Doc.254 that addresses these issues so that defense testing is actually possible and can be completed in a safe and secure manner for both the government and the defense.

DATED at Anchorage, Alaska, this 25th day of November 2019.

THE LAW OFFICES OF ROBERT HERZ, PC

s/ Robert M. Herz
431 W. 7th Avenue, Suite 107
Anchorage, Alaska 99501
Phone 907-277-7171
Fax 907-277-0281
rmherz@gci.net
AK Bar No. 8706023

CERTIFICATE OF SERVICE
I hereby certify that on Nov 25, 2019, a copy of the foregoing Def M for Partial Reconsideration was served electronically on Assistant United States Attorney's Office s/ Robert Herz