BRYAN SCHRODER
United States Attorney

JONAS M. WALKER
CHARISSE ARCE
Assistant U.S. Attorneys
Federal Building & U.S. Courthouse
222 West Seventh Avenue, #9, Room 253
Anchorage, Alaska 99513-7567
Phone: (907) 271-5071
Fax: (907) 271-1500
Email: jonas.walker@usdoj.gov
charisse.arce@usdoj.gov

Attorneys for Plaintiff

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF ALASKA

UNITED STATES OF AMERICA, Plaintiff, vs. MATTHEW WILLIAM SCHWIER, Defendant.	)	No. 3:17-cr-00095-SLG

MOTION FOR PARTIAL RECONSIDERATION REGARDING ORDER (Dkt. 254) AND FOR TELEPHONIC PARTICIPATION OF WITNESS AT STATUS HEARING

The United States, by undersigned Assistant United States Attorney, pursuant to L.Civ.R. 7(h)(1)(A), respectfully moves the Court for partial reconsideration of the Order Re Motion for Additional Terms for Protective Order (Dkt. 244) (the "Order," Dkt. 254), and pursuant to L.Civ.R. 7(i), telephonic participation by a witness. The government

respectfully requests an opportunity to present the testimony of a witness to explain the issues discussed below.

In the 14 days since the Court originally ordered the government to make Torrential Downpour available to the defense (Dkt. 243), the government has diligently worked to craft an appropriate protective order that complies with both United States v. Budziak, 697 F.3d 1105 (9th Cir. 2012), and Roviaro v. United States, 353 U.S. 53 (1957). In an unprecedented development, the United States has agreed to allow a defense expert to test Torrential Downpour outside the presence of a government agent. The government has, in good faith, rapidly proposed two protective orders. Taking into account the defense's objections to the first proposed order (244-1), the government crafted a second proposed protective order (253-4) that allowed internet access, but required Wireshark as a way to protect the software from copying.

A) Wireshark provides some assurance against software copying, but imposes no costs on the defense.

The Court held (Order at 2) that FRCrP 16 does not impose a duty on the defense to preserve evidence. The government does not dispute this legal conclusion.

However, the Order overlooked, and did not address, an important reason the government seeks a protective order with Wireshark or another appropriate packet-capture software: *i.e.* detecting digital copying of Torrential Downpour from the TD Computer.

Put another way: there are two potential ways that Torrential Downpour could be compromised at the OCRCFL; first, being physically removed from the OCRCFL; or, second, which is more likely to occur, being digitally copied from the TD Computer onto

other media. The Court has adequately protected Torrential Downpour from being physically removed from the OCRCFL by ordering that the defense will not open, tamper with, or remove the TD Computer from the OCRCFL.

However, the Order provides no way to verify that Torrential Downpour has not been copied from the TD Computer. The risk is that, during testing, the defense could inadvertently copy Torrential Downpour onto the digital media or computers that will be brought into the room with the TD computer. Copying Torrential Downpour would be as easy as copying any file. To be clear, the government is not accusing the defense of intending violate a protective order, or conspiring to violate 18 U.S.C. § 1030, or otherwise attempting to copy the software from the TD Computer. Rather, the government is seeking a reasonable prophylactic measure that will confirm that the software has not been copied.

Mr. Fischbach has, already, lost a hard drive at the OCRCFL in this case. *See* Dkt. 253-2 (email from Joe Monroe, stating "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").[1] Given the high importance of protecting Torrential Downpour from disclosure, such negligence is reasonable cause for concern, particularly in light of the government's evidence that Torrential Downpour must be protected from disclosure.

> The government presented similar evidence in this case, which the Court finds persuasive. Robert Erdely—offered by the government as an expert—stated in his declaration that "child pornography distributors could find a way to avoid detection" if the workings of Torrential Downpour were made

1 The government's understanding is that Mr. Fischbach insinuated that the OCRCFL was at fault.

> public, rendering that tool of law enforcement ineffective. At the evidentiary hearing, Mr. Erdely testified that to give the defense unfettered access to this software puts law enforcement and ten years of development at risk because it would reveal certain aspects of Torrential Downpour's operation.

Dkt. 231 at 9-10 (internal punctuation omitted).

Moreover, given his purported experience with classified information, Mr. Fischbach should be comfortable complying with procedures intended to verify that sensitive information is not inadvertently lost during discovery. Indeed, that is the very purpose of the OCRCFL.

Finally, Wireshark provides significant protections for the government, but imposes no costs on the defense. Wireshark will not interfere with any privileged information, because the government will not possess the Wireshark data. Wireshark will not interfere with any testing the defense runs.

The government respectfully requests a status hearing with an opportunity to present the telephonic testimony of a witness who can explain the security value of Wireshark.

B) The government is working to comply with other aspects of the Order (Dkt. 254).

The government has identified a computer with specifications similar to the one already in use in this case. Per Mr. Herz's email at Dkt. 253-3, such a computer should satisfy the defense.

The Court ordered the government to "provide the defense with all applicable TD software documentation for versions 1.15 and 1.23, including installation instructions and minimum operating requirements" by the end of one working day. Order at 254. The Court did not define "all applicable TD software documentation." The government is diligently

working to identify a manual for those two versions of Torrential Downpour and redact the privileged information therefrom for discovery.

C) Conclusion

The government respectfully requests the Court schedule a status hearing on November 25 or 26, 2019, at which the government may present the testimony of a witness to briefly explain why Wireshark (or another packet capture program) is important to protect Torrential Downpour from being compromised during testing. In the event that the Court rejects the use of any packet-capture software, the government may request an additional period to propose an alternative technical arrangement that would permit the defense to do testing.

RESPECTFULLY SUBMITTED November 22, 2019, in Anchorage, Alaska.

BRYAN SCHRODER
United States Attorney

s/ Jonas M. Walker
JONAS M. WALKER
Assistant U.S. Attorney
United States of America

CERTIFICATE OF SERVICE

I hereby certify that on November 22, 2019,
a true and correct copy of the foregoing
was served by served through ECF on:

Robert Herz

s/ Jonas M. Walker
Office of the U.S. Attorney