

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,            ) No. 3:17-cr-00095-SLG  
  ) )  
  Plaintiff,            ) )  
  ) )  
  vs.                         ) )  
  ) )  
MATTHEW WILLIAM SCHWIER,            ) )  
  ) )  
  Defendant.            ) )  
\_\_\_\_\_ )

**MOTION FOR ADDITIONAL TERMS FOR PROTECTIVE ORDER AND  
NOTICE OF COMPLIANCE WITH SUPPLEMENTAL ORDER (Dkt. 243)**

The United States, through undersigned Assistant U.S. Attorney, responds to the Supplemental Order Regarding C-3 Motion to Compel Discovery and Production of Evidence: Torrential Downpour (the “Order,” Dkt. 243). As explained below, the government has been working diligently to meet the Order’s one-week deadline, and the computer can be available on November 20, 2019.

**A) The government elects to provide limited access to a computer running  
Torrential Downpour, rather than dismiss Counts 1 and 2.**

The Order permits the government to choose between only two options: first, allowing the defense to perform four tests on Torrential Downpour, the nature of which are withheld from the government; or, second, dismissing Counts 1 and 2.<sup>1</sup> The Order is silent regarding technical aspects of how the government must provide the computer.

In the event the Court orders the additional terms of the protective order, below, the government is electing to provide access consistent with the Order, rather than dismissing Counts 1 and 2. The government is selecting this option because the Order does not compel internet access for the computer; nor does it permit the defense to add or remove software or hardware from the computer; nor does it allow the computer to leave the Orange County Regional Computer Forensics Lab (OCRCFL).<sup>2</sup> Most importantly, and consistently with the Court's prior protective order at Dkt. 231, the Order does not result in the software itself being released into "the wild." Finally, the Order leaves in place the broad protective language in Dkt. 231.<sup>3</sup> Thus, the order strikes a "proper balance" between production and

---

<sup>1</sup> "The government may opt to dismiss Counts 1 and 2; if it does so, it is not required to further produce the Torrential Downpour software to the defense. In that event, the government may still proceed on Count 3." Order, Dkt. 243, at 7.

<sup>2</sup> The OCRCFL is located at 3800 W. Chapman Avenue, Suite 800, Orange, CA 92868. *See* Order Re: Compliance With Discovery Procedure, Dkt. 158 at footnote 4 regarding referring to the OCRCFL as the "Anaheim RCFL."

<sup>3</sup> The Court ordered:

Defense counsel and defense expert may not disclose their notes, the information contained in the notes, or any other information relating to their observation of the Torrential Downpour validation process or subsequent forensic examination of the computers involved therein to any person other

protection Roviaro v. United States, 353 U.S. 53 (1957).

Accordingly, the government is preparing a computer for defense access at the OCRCFL. The government will take reasonable measures to ensure that the computer will not access the internet, for several reasons. First, the Court did not order internet access. *See* Order, Dkt. 243. Second, because Torrential Downpour is designed to, and does reliably, download child pornography, connecting it to the internet would create a risk that it would fulfill its intended function, thereby facilitating the distribution of child pornography, in violation of 18 U.S.C. § 2252A, and other applicable laws, which the Order does not permit. Third, the Court did not order the defense to have access to ICAC COPS, which could be accessible via the internet. Likewise, the government will take reasonable measures to ensure that Torrential Downpour cannot be digitally or physically removed from the computer.

**B) Additional terms for a protective order**

Pursuant to paragraph (2) of the Order at Dkt. 243 at 7, the government respectfully requests the Court order the following additional terms to a protective Order:

1. The government will provide a computer at the OCRCFL. The computer will have one version of Torrential Downpour installed, *i.e.*

---

than each other. Any information, data, and notes derived from the defense's observation of the validation process or its subsequent forensic examination shall be used solely for the purpose of conducting proceedings in this case and for no other purpose whatsoever. It shall not be disseminated to any other person without prior order of the Court.

Dkt. 231 at 13.  
U.S. v. Schwier  
3:17-cr-00095-SLG

version 1.23, one of the versions used in this investigation. The Torrential Downpour software installed will not have access to law enforcement's database of hash values from known child pornography images.

2. The only persons who will have access to the computer are Jeffrey Fischbach and Robert Herz (collectively "the defense"). The defense will have access to the computer for 21 consecutive days of testing.
3. The computer will contain one network card. The defense will not make any connections to this computer other than through the network card.
4. The defense may bring digital media, computers, and phones into the room with the computer.
5. The defense will not remove the computer from the OCRCFL. The defense will not copy Torrential Downpour.
6. The computer will be sealed with evidence tape. Other than the network card, all other ports/connections to the computer will be sealed with evidence tape. The defense will not tamper with or open the computer, nor break or remove the evidence tape.
7. The defense will not download or distribute child pornography using the computer. Any downloading of child pornography would constitute a violation of the federal criminal code.

8. All communications with the Torrential Downpour computer will be preserved via Wireshark. This preservation includes all communications with the computer containing Torrential Downpour during the 21 days of testing, both communications during testing and at all times the computer is powered up. The defense shall maintain the Wireshark data pending further order of the Court.
9. At the conclusion of testing, the FBI will “zip” all the Wireshark files, meaning it will use software to compress them. The FBI will “hash” the zipped file(s), burn the zipped file(s) to a disk(s), sign the disk(s), and provide the disk(s) to the defense to maintain said disk(s) until further order by the Court. Both the defense and the FBI will be provided the hash values associated with these Wireshark file(s). However, the government will not possess the disk(s) themselves. At the conclusion of this matter, the Court will order the destruction of all copies of the disks, under circumstances to be determined, in order to prevent dissemination of the data thereon.

The government believes that these restrictions should permit the defense to perform any legitimate testing on Torrential Downpour, while, also, ensuring that the software is not removed from the computer.

The Court is familiar with Wireshark; it is the screen-recording and packet-capturing program the government used during the validation testing previously ordered

by the Court.<sup>4</sup> For the current testing, the preservation of Wireshark data accomplishes two goals. First, it creates some measure of protection against the copying of Torrential Downpour. Second, it protects the integrity of the testing process. To the extent that Mr. Fischbach testifies pursuant to FRE 702, the Wireshark data would be the best possible evidence regarding the testing.

**C) Objections to defense's *ex parte* advocacy.**

In an abundance of caution, and to preserve the record, the government notes that, on record on November 4 and 5, 2019, prior to the Court issuing the Order, the government objected to the Court's consideration of the defense's *ex parte* communication. *See* Dkt 234-1 (redacted version of Mr. Fischbach's declaration). The government respectfully maintains its objections to the Court's consideration of the defense's *ex parte* communications.

On October 17 and 18, 2019, the parties' expert witnesses testified at length. Following that hearing, the Court ordered the government's proposed testing and denied the defense's request that the government produce Torrential Downpour. Dkt. 231. This order made sense in light of the defense's failure to identify the tests and Mr. Fischbach's performance under cross-examination.<sup>5</sup>

Having failed to meet its burden under Budziak at the evidentiary hearing, the defense later submitted, *ex parte*, a Declaration of Jeffrey M. Fischbach, dated October 31,

---

<sup>4</sup> *See* Dkt. 219-1 at para. 3; Dkt. 231 at 12.

<sup>5</sup> "But when asked about the materiality of this information, Mr. Fischbach was only able to speak in vague generalities, claiming attorney-client privilege." Dkt. 231 at 11.

2019, a redacted version of which the government received at Dkt. 234-1. As the Court notes in the Order, “[i]n the redacted copy of Mr. Fischbach’s declaration, the entire description of these four tests and their relevance to the defense are blacked out.” Order at 243 at 6. Thus, it was not until October 31 that the defense identified the tests, long after the government’s opportunity to challenge the merits of Mr. Fischbach’s claims had passed. In this way, the defense achieved, via *ex parte* advocacy, that which it failed to do when Mr. Fischbach was subject to cross-examination in open court.

“[I]n our system, adversary procedures are the general rule and *ex parte* examinations are disfavored.” United States v. Kenney, 911 F.2d 315, 321 (9th Cir. 1990). The “reliability [of evidence is] assessed in a particular manner: by testing in the crucible of cross-examination.” Crawford v. Washington, 541 U.S. 36, 61 (2004). “This open examination of witnesses is much more conducive to the clearing up of truth” because “adversarial testing beats and bolts out the Truth much better.” Id. (internal citations and punctuation omitted). The Supreme Court has described cross-examination as the “greatest legal engine ever invented for the discovery of truth.” Maryland v. Craig, 497 U.S. 836, 846 (1990).

Due to the *ex parte* nature of the defense’s advocacy, the government is ignorant of the four tests, their procedures, goals, scientific validity, and technological requirements. Accordingly, the government has had no opportunity to contest their materiality under United States v. Budziak, 697 F.3d 1105 (9<sup>th</sup> Cir. 2012). As the Court has already

acknowledged<sup>6</sup>, the government has a legitimate interest in protecting Torrential Downpour, pursuant to Roviaro v. United States, 353 U.S. 53 (1957). The government’s interest in protecting, and responsibility to protect, this important tool for investigating child pornography is especially heightened when, as here, the government has been kept ignorant of the tests that the defense is requesting.

Moreover, the secrecy of the tests has complicated the government’s response to the Order. Due to the nationwide importance of protecting Torrential Downpour, while also effectively prosecuting child pornography offenses, the decision regarding how to respond to the Order is not solely that of the U.S. Attorney’s Office for the District of Alaska. Accordingly, in the four working days since the Court issued the Order, the government has conferred with the FBI Office of General Counsel; the Child Exploitation and Obscenity Section of the Criminal Division of the U.S. Department of Justice; another U.S. Attorney’s Office; in addition to personnel involved in this investigation.

//

---

<sup>6</sup> The Court held:

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 public, “render[ing] 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.

Order Regarding C-3 Motion, Dkt. 231 at 10-11.

U.S. v. Schwier  
3:17-cr-00095-SLG

**D) Conclusion: The computer will be available by November 20, 2019.**

The FBI has advised the undersigned that it can have the computer prepared and in place at the OCRCFL, ready for the defense, by Wednesday, November 20, 2019. The government respectfully requests the Court issue the attached protective order, the terms of which are essential to protect Torrential Downpour, and which should not interfere with any testing by the defense. Absent these protections, the government cannot provide the computer.

The government objects to any additional *ex parte* advocacy by the defense, particularly regarding the terms of the protective order. If necessary, the government can provide an affidavit, or the testimony of a witness, to explain the merits of the terms of the protective order.

RESPECTFULLY SUBMITTED November 15, 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 15, 2019, a true and correct copy of the foregoing was served electronically on the following:

Robert M. Herz

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

U.S. v. Schwier  
3:17-cr-00095-SLG