IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

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

ORDER RE MOTIONS FOR RECONSIDERATION

Before the Court at Docket 255 and Docket 256 are the government and the defense's respective Motions for Partial Reconsideration of the Court's order at Docket 254.

BACKGROUND

The factual background of this case is well known to the parties and is condensed here as relevant to the pending motions. On September 12, 2019, the defense filed a motion seeking the production of the Torrential Downpour software.[1] On October 17 and 18, 2019, the Court heard extensive testimony from government and defense experts regarding the materiality of independent defense testing of the Torrential Downpour software. On October 24, 2019, the Court entered an order that granted in part and denied in part the defense's motion

[1] Docket 199.

to compel production of Torrential Downpour.[2] The Court there found that the functionality, reliability, and accuracy of Torrential Downpour were material to Mr. Schwier's defense,[3] but that a validation test performed by the government would be "sufficient to meet the defense's needs" under the balancing test set forth in *Roviaro v. United States*, 353 U.S. 53 (1957).[4]

However, the Court's October 24, 2019, order allowed the defense to file a supplemental declaration of its expert to explain why it believed that additional testing was necessary, and the Court notified the parties that it may amend its order in light of that declaration.[5] On October 31, 2019, the defense filed a supplemental ex parte declaration of Jeffrey M. Fischbach, which described four additional tests he sought to conduct with the Torrential Downpour software.[6] The defense filed a redacted copy of Mr. Fischbach's declaration on the same day, from which it had removed all information claimed as privileged, including the entire

---

[2] Docket 231; *see also* Docket 199 (motion).

[3] Docket 231 at 7–8.

[4] Docket 231 at 10–11. *Roviaro* directs courts determining whether to apply the law enforcement privilege to balance the public interest against the defendant's right to prepare his defense, "taking into consideration the crime charged, the possible defenses, the possible significance of the informer's testimony, and other relevant factors." 353 U.S. at 62.

[5] Docket 231 at 12, 14.

[6] Docket 233.

description of the four tests.[7]

On the government's motion,[8] the Court held a brief status conference on November 4, 2019, after which the parties conducted validation testing of Torrential Downpour pursuant to the October 24, 2019 order.[9] The Court held a second status conference the next day, and on November 8, 2019, ordered the production of Torrential Downpour for defense testing at the Orange County Regional Computer Forensics Lab ("OCRCFL"), "limited to the four tests described in Mr. Fischbach's October 31, 2019 declaration."[10]

The Court's November 8, 2019, order allowed the government to "propose additional terms to the protective order entered at Docket 231 as warranted."[11] The government did so on November 15, 2019,[12] and after yet more briefing, on November 22, 2019, the Court entered a supplemental protective order to govern the defense's testing of the Torrential Downpour software.[13] The order required

[7] Docket 234.

[8] Docket 235.

[9] Docket 243 at 2.

[10] Docket 243 at 2, 7–8.

[11] Docket 243 at 8.

[12] Docket 244. The defense's Response in Opposition is at Docket 248, and the government's Reply is at Docket 253.

[13] Docket 254. The original protective order is at Docket 244.

the government to provide a computer to run Torrential Downpour (the "TD Computer"), while the defense could bring its own computers to connect to the TD Computer with an internet hotspot.[14] Paragraph 6 of the order provided that "[g]overnment 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 [C]omputer secure consistently with OCRFCL standard operating procedures."[15] Paragraph 7 required Mr. Fischbach to install Torrential Downpour onto the TD Computer in the presence of an "FBI agent or Task Force Officer."[16] Paragraph 9 provided that "[t]he TD Computer will contain one network card," and that "[t]he defense will not make any connections to the TD Computer other than through the network card."[17] The November 22, 2019 order did not require the defense to use the packet capture program WireShark during its testing of Torrential Downpour.[18]

The government filed a Motion for Partial Reconsideration at Docket 255,

[14] Docket 254 at 3, 5.

[15] Docket 254 at 4.

[16] Docket 254 at 4.

[17] Docket 254 at 5. Paragraph 8 of the November 22, 2019, Protective Order specified that the defense would be required to connect to the TD Computer using an internet hotspot "that is compatible to connect to the TD Computer via the network card." Docket 254 at 5.

[18] Docket 254 at 2.

requesting that the Court require the defense's use of "Wireshark or another appropriate packet-capture software" to detect whether Torrential Downpour had been copied from the TD Computer.[19]

The defense filed its own Motion for Partial Reconsideration at Docket 256, requesting that the Court amend the November 22, 2019, order to allow Mr. Fischbach to enter the password on the TD Computer himself, install Torrential Downpour without supervision, and to "connect to the TD . . . Computer as necessary to complete its testing."[20]

The Court held a hearing on the parties' cross-motions for partial reconsideration on November 26, 2019. At the hearing, the Court ordered the government to file a response to the defense's motion after it had consulted with the FBI.[21] The Court emphasized at that hearing that it was "not asking the government to propose additional testing," but rather was asking the government "to respond to the defense motion for reconsideration . . . and tell [the Court] what you disagree with and agree with."[22] The Court further explained it sought for the

[19] Docket 255 at 2–4.

[20] Docket 256; Docket 256-1 at 2–3 (proposed order).

[21] Docket 302 at 6:22–9:9.

[22] Docket 302 at 7:15–19.

government "to respond to this issue of WiFi versus Ethernet, the issue of how many access . . . ports into the computer, the issue of the copying as articulated here, and tell me what the government's position is on those."[23] The government responded that the "subject matter experts at the [FBI] . . . [would] need until December 13th to come up with that."[24]

The Court's instructions notwithstanding, the government on December 20, 2019, filed a status report that attached an entirely new proposed testing protocol.[25] As correctly observed by the defense, in filing this proposed new protocol, some three months after the defense motion was filed, and two months after the evidentiary hearing, "[t]he government has seemingly repudiated the testing protocol as provided for in the Court's orders at 231, 243, and 254 the terms of which the government previously had agreed to."[26] The author of the proposed new protocol is not identified; it appears to have been created by one or more

[23] Docket 302 at 8:7–11.

[24] Docket 302 at 8:14–17.

[25] Docket 288. The government's filing incorrectly states "[a]t the hearing on November 26, 2019, the Court ordered the government to submit a revised protective protocol." Docket 288 at 2. By filing a new proposed testing protocol with its response to the defense's Motion for Partial Reconsideration, a full two months after the initial evidentiary hearing regarding defense testing of Torrential Downpour, the government disregarded the Court's clear instruction on the record to restrict its filing to a direct response to the defense's reconsideration motion.

[26] Docket 296 at 2.

unidentified FBI agents.[27] The government states that it is willing to provide testimony from unidentified person(s) to explain its new proposal.[28] The defense filed a response to the government's filing at Docket 296 and an accompanying Supplemental Declaration of Mr. Fischbach at Docket 297. Given this record, the Court declines to consider the government's newest proposed protocol.

Separately, December 19, 2020, the government filed a Fourth Superseding Indictment in the case.[29] The new indictment adds a fourth count to the charges against Mr. Schwier: receipt of child pornography on or about November 18, 2015.[30]

DISCUSSION

The Court will address the parties' respective motions for reconsideration separately, beginning with the defense's motion at Docket 256.

1. Defense's Motion at Docket 256

The defense contends that the November 22, 2019, Protective Order

[27] *See* Docket 288-1 at 1 ("[T]he FBI determined the following test conditions are necessary to sufficiently protect the software from unauthorized disclosure.").

[28] Docket 288 at 2. In a January 13, 2020, Status Report, the government clarified that it would present Detective Erdely "to provide expert testimony regarding the [proposed] Test Environment." Docket 303 at 2.

[29] Docket 279.

[30] Docket 279 at 3.

contains three "manifest error[s] of fact."[31] The defense argues that the first of these is "paragraph 9[,] which limits the defense to the use of one port and network connection" on the TD Computer.[32] The defense maintains that this paragraph prohibitively limits Mr. Fischbach's ability to complete his testing of the software by "prevent[ing] him from installing industry accepted software and hardware as well as well as prevent[ing] him from removing his test results from the [TD Computer] for further examination and analysis on his own equipment."[33] And Mr. Fischbach states in his declaration that he "need[s] access to multiple computer ports and network connections to run [his] tests."[34] The government does not meaningfully respond to the defense's argument. It contends only that the defense's argument is moot in light of the government's new proposed testing protocol, which would allow the defense "to use screens, keyboards, and mice."[35]

Mr. Fischbach, in his declaration, persuasively explains why he requires access to multiple ports on the TD Computer in order to complete the testing

---

[31] Docket 256 at 1–3; *see* L. R. Civ. P. 7.3(h)(1)(A) ("A court will ordinarily deny a motion for reconsideration absent a showing of . . . [a] manifest error of the law or fact.").

[32] Docket 256 at 2.

[33] Docket 256 at 2.

[34] Docket 257 at 8, ¶ 5(e); *see also id.* at 2, ¶ 2.

[35] Docket 288 at 3–4. As noted above, the Court declines to address the new protocol, which it considers to be improperly filed.

authorized by previous order of this Court.[36] And the government has not explained how restricting the defense's access to ports on the TD Computer is necessary to protect Torrential Downpour's integrity as a law enforcement tool. The Court will therefore grant the defense's motion to reconsider with respect to paragraph 9 of the November 22, 2019, protective order.

The defense next argues that "Paragraphs 6 and 7 of the . . . [November 22, 2019,] order . . . compromise attorney-client privilege and attorney work product by intruding upon the confidential and independent defense testing process."[37] The defense contends that Paragraph 6's provision that government personnel start and enter the password on the TD Computer "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 [Torrential Downpour] software or his own results as the government now has access to defense work product."[38] The defense maintains that "the only person who should have sole access to defense work product is Mr. Fischbach, and as such he should have sole and exclusive

[36] Docket 257 at 8, ¶ 5(e); *see also id.* at 2, ¶ 2.

[37] Docket 256 at 3. "The work-product doctrine protects 'from discovery documents and tangible things prepared by a party or his representative in anticipation of litigation.'" *United States v. Richey*, 632 F.3d 559, 567 (9th Cir. 2011) (quoting *Admiral Ins. Co. v. U.S. Dist. Ct.*, 881 F.2d 1486, 1494 (9th Cir. 1989)).

[38] Docket 256 at 3.

possession of any passwords."[39] In his declaration, Mr. Fischbach explains that under the terms of Paragraph 6, the personnel responsible for powering on and logging into the TD Computer "would be able to see my examination progress each time they have to log me back into the system . . . , as well as hold exclusive possession of the password to access it while I am away."[40]

The defense further maintains that the way that Mr. Fischbach configures the TD Computer would reveal to a knowledgeable observer information about the type of testing he plans to conduct.[41] The defense therefore contends that Paragraph 7's provision that an FBI agent may observe Mr. Fischbach install Torrential Downpour onto the TD Computer risks divulging privileged information.[42] Mr. Fischbach states in his declaration that "[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."[43]

The government argues in its response that the defense's assertion of

---

[39] Docket 256 at 3.

[40] Docket 257 at 4, ¶ 5(a).

[41] Docket 256 at 3.

[42] Docket 256 at 3–4.

[43] Docket 257 at 4, ¶ 5(a); *see also id.* at 6, ¶ 5(b) (Mr. Fischbach explaining that configuration of TD Computer would occur before installation of Torrential Downpour and "necessarily make the observing agent privy to attorney client privilege").

privilege is deficient because "Torrential Downpour is the government's software"; because "the presence of the computers and software at the OCRCFL [and] Mr. Fischbach's use of them to prepare for trial . . . are not privileged information"; and because Mr. Fischbach had previously referred to his testing methods as adhering to the "industry standard."[44] The government's argument misses the mark. The defense does not claim that Torrential Downpour itself or the mere use of computers or software at OCRCFL constitute privileged work product. Rather, the defense asserts privilege regarding the tests Mr. Fischbach will perform on Torrential Downpour using that hardware and software.[45] The nature of the tests that Mr. Fischbach intends to conduct on Torrential Downpour and the results thereof are clearly privileged.[46] As the government itself notes, "[t]he work-product doctrine covers documents or the compilations of materials prepared by agents of the attorney in preparation for litigation."[47]

---

[44] Docket 288 at 6–7.

[45] Docket 296 at 8–9.

[46] The Court does not understand Mr. Fischbach to have asserted that the tests themselves were standard, but rather that they complied with industry-accepted standards. *See* Docket 296 at 9.

[47] Docket 288 at 4 (quoting *United States v. Richey*, 632 F.3d 559, 567 (9th Cir. 2011)); *see also Hernandez v. Tanninen*, 604 F.3d 1095, 1100 (9th Cir. 2010) ("The work product doctrine is a qualified privilege that protects certain materials prepared by an attorney acting for his client in anticipation of litigation.").

Mr. Fischbach has persuasively explained that granting the government exclusive password access to the TD Computer and allowing government agents to observe his configuration of that computer would compromise privileged attorney work-product. The government has not introduced evidence to the contrary and maintains only that password-protection is necessary to prevent "the defense from bypassing certain," unspecified, "protections by powering down the computer and then restarting testing without the protections being activated."[48] The Court finds this vague and unsupported assertion unconvincing and will grant the defense's motion with respect to Paragraphs 6 and 7 of the November 22, 2019, Protective Order.

Finally, the defense contends that Paragraph 8's requirement that Mr. Fischbach utilize "an internet hotspot . . . that is compatible to connect to the TD Computer via the network card," is erroneous because "[t]here is no valid basis to restricting the defense to a wired Ethernet connection."[49] The defense requests an amendment allowing Mr. Fischbach to connect to the TD Computer using a standard WiFi connection.[50] The government explained at the November 26,

[48] Docket 288 at 2–3.

[49] Docket 256 at 4.

[50] Docket 256 at 4.

2019, hearing that the term requiring an ethernet connection had been proposed "because [the government's] understanding is it would not be possible for [Mr. Fischbach] to use WiFi at the RCFL," and that "[t]he intent was to identify for him what he would need to do to connect."[51] The Court concludes from this that Paragraph 8's Ethernet requirement serves no valid security purpose, and will therefore grant the defense's motion with respect to the use of WiFi to connect to the TD Computer, to the extent that it is possible to establish a WiFi connection under the OCRCFL's normal operating procedures.

2. Government's Motion at Docket 255

The November 22, 2019, Protective Order did not require the defense to use WireShark during its testing of Torrential Downpour. The Court there explained:

> The government proposes that the protective order contain a term providing that "[a]ll communications with the Torrential Downpour computer will be preserved via Wireshark." The defense objects, contending that "[t]he [C]ourt has no more authority under Criminal Rule 16 to impose a duty on the defense to create evidence than it has to impose such a duty on the government." The Court agrees with the defense on this point, and will not order the defense to use WireShark during its testing of Torrential Downpour.[52]

In its Motion for Partial Reconsideration, the government argues that the protective order "overlooked, and did not address, an important reason the government seeks

[51] Docket 302 at 6:13–18.

[52] Docket 254 at 2 (internal citations omitted).

a protective order with Wireshark or another appropriate packet-capture software: *i.e.* detecting digital copying of Torrential Downpour from the TD Computer."[53]

The Court recognizes the government's concern that "the defense could inadvertently copy Torrential Downpour" onto their own equipment but will not grant the government's motion on this basis. However, the Court finds Mr. Fischbach to be responsible and in possession of technical expertise such that he would be unlikely to unwittingly copy Torrential Downpour and remove it from the OCRCFL.[54] And the Court has expressly ordered the defense not to copy Torrential Downpour and expects compliance with that order. The Court sees no reason to revisit its decision regarding WireShark and will therefore deny the government's Motion for Partial Reconsideration.

3. Miscellaneous Issues Raised in the Government's Response

In addition to responding to the defense's motion for partial reconsideration, the government's response at Docket 288 raises several additional issues. For reasons set out above, the Court will not here consider the government's new

[53] Docket 255 at 2.

[54] A supplemental declaration filed by Mr. Fischbach indicates that the government, itself, believes him to be trustworthy. Mr. Fischbach states that the government inadvertently included two copies of Torrential Downpour on a thumb drive it provided to him on December 6, 2019. Docket 297 at 2, ¶ 2. Mr. Fischbach states that the government, upon realizing this, took no action besides reminding him not to copy the software from the thumb drive. Docket 297 at 2–3, ¶¶ 4–5.

testing protocol, which it proposed a full two months after the Court's first evidentiary hearing regarding the proper environment for defense testing of Torrential Downpour; the Court will, however, address the remaining issues here.

a. Specifications of TD Computer

The November 22, 2019, Protective Order clearly outlines the procedure by which the specifications for the TD Computer would be established. The order first requires 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*."[55] The order next requires the defense to "provide the specifications for the computer that it is seeking for TD testing."[56] Finally, the order requires the government to "provide a government-owned computer . . . that is configured to specifications that were timely provided by the defense."[57] Only "[i]f the defense fails to timely provide such specifications," may "the government . . . select the computer it will provide."[58]

On November 25, 2019, the government provided the defense with a

[55] Docket 254 at 2.

[56] Docket 254 at 2–3.

[57] Docket 254 at 3.

[58] Docket 254 at 3.

redacted user manual for Torrential Downpour version 1.23.[59] Despite the defense's arguments to the contrary,[60] the Court finds that this user manual fulfilled the government's obligation to provide the defense with Torrential Downpour's minimum operating requirements.[61] On December 6, 2019, the Defense timely complied with its obligation to provide the government with system specifications for the TD Computer.[62] Under the terms of the November 22, 2019, Protective Order, the government is now required to provide the defense with a computer that is configured to the specifications supplied by the defense.[63]

The government nevertheless objects to the defense's technical specifications, maintaining that at the November 26, 2019, hearing, "the Court ordered the government to respond to the defense's objections to the computer

[59] *See* Docket 259 (Government's Notice Regarding Partial Compliance with Order (Dkt 254 and Correction of Record). The parties dispute the appropriateness of the government's redactions, *see* Docket 282 (Defense's C-5 Motion to Compel), an issue which the Court will address in a separate order after reviewing the relevant materials in camera.

[60] *See* Docket 296 at 12 n.9 ("The government's claim that it provided software specifications seems disingenuous at best.").

[61] Docket 299-1 at 8 (identifying operating system and programming model required to run Torrential Downpour).

[62] Docket 281-2 at 4. At the November 26, 2019, hearing, the Court extended the deadline to provide these specifications from November 27, 2019, to December 6, 2019. Docket 302 at 10:1–13.

[63] Docket 254 at 3.

the government will provide for testing."[64] The Court disagrees, but has reviewed the transcript for that hearing and understands how the government reached that conclusion.[65] It will therefore address the government's arguments. The government contends that the defense's specifications "are not necessary to operate Torrential Downpour or uTorrent software and to conduct the types of industry-standard tests that the government expects the defense will perform."[66] The government therefore asserts that the defense's specifications "are unreasonable."[67] The government provides no evidence, in the form of a declaration or otherwise, to support its contentions.

As the defense notes, the purpose of the TD Computer is to *test* Torrential Downpour, not to operate it.[68] It is therefore understandable that Mr. Fischbach would require more computing power than is necessary to simply operate the

---

[64] Docket 288 at 9.

[65] Docket 302 at 2:5–5:20.

[66] Docket 288 at 11.

[67] Docket 288 at 10. The government further maintains that "[b]ecause the defense has withheld from the government the specific characteristics of its proposed testing, the government cannot know with certainty what the defense's actual requirements are." Docket 288 at 10. This argument misunderstands the November 22, 2019 order; that order requires the government to provide a computer consistent with the specifications supplied by the defense, not consistent with what the government determines "the defense's actual requirements are." Docket 254 at 2–3.

[68] Docket 296 at 12–13.

software. Mr. Fischbach explains in his declaration that he "specifically chose[]" the specifications to "accommodate the forensic hardware and software [he] need[s] to install in order to both complete [his] testing and assure the [C]ourt that the machine has in no way been compromised during [his] testing, and that no software has been lost, stolen, or compromised."[69] On this record, the Court finds that the specifications provided by the defense on December 6, 2019, are not only necessary for Mr. Fischbach to conduct his testing of Torrential Downpour, but also promote the government's interest in ensuring that the testing is secure.

The Court will therefore order the government to provide the defense with a computer that is configured to the specifications identified at Docket 280-1 page 1, pursuant to the November 22, 2019, Protective Order.

b. Location of Testing

At the November 26, 2019, hearing, the Court directed the government to address whether the defense's testing of Torrential Downpour could occur at the Sensitive Compartmented Information Facility ("SCIF") at the federal building and courthouse in Los Angeles instead of the OCRCFL.[70] Having reviewed the

[69] Docket 261 at 7, ¶ 8.

[70] Docket 302 at 9:13–18.

parties' briefing on this issue,[71] the Court finds that it would not be appropriate to relocate testing to the SCIF. The defense notes that "the government has not raised any objection to moving the testing location to the FBI-Wilshire office," which it asserts "would be a more secure location than the RCFL."[72] If the parties can agree to relocate testing to the FBI-Wilshire office, they can notify the Court and the Court will so order. Unless and until such an agreement is reached, testing will be at the OCRCFL.

CONCLUSION

In light of the foregoing, the government's Motion for Partial Reconsideration at Docket 255 is DENIED. The defense's Motion for Partial Reconsideration at Docket 256 is GRANTED.

The Court will separately issue an amended protective order consistent with this decision.

DATED this 13th day of January, 2020, at Anchorage, Alaska.

s/ Sharon L. Gleason
UNITED STATES DISTRICT JUDGE

[71] *See* Docket 288 at 7–9; Docket 296 at 9–10.

[72] Docket 296 at 10.