UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA, v. ROMAN STERLINGOV, *Defendant.*	Criminal Action No. 21-399 (RDM)

MEMORANDUM OPINION AND ORDER

On November 4, 2023, the Court issued a decision addressing whether the supplemental protective order in this case, Dkt. 196, should be construed to restrict the defendant, Roman Sterlingov, from personally reviewing the covered material. *See* Dkt. 210. As explained in that decision, the supplemental protective order covers the sensitive, supplemental heuristic information that was created by the government's expert (for the benefit of the defense) and provided to the defense in September 2023. *See id.* at 1; Dkt. 196. At the time of the Court's November 4 decision, the Court was unable to determine from the parties' prior briefing: (1) whether the government had met its burden of demonstrating good cause to deny Sterlingov access to that information; (2) whether any such good cause justification extended to the entire sensitive, supplemental production or only to parts of it; and (3) whether Sterlingov was seeking access to the material because he had relevant expertise that might assist his counsel in preparing his defense or whether, instead, he merely sought access as a matter of principle. Dkt. 210 at 2.

Having reviewed the parties' filings, Dkt. 206; Dkt. 207, and having considered their representations at the November 13, 2023 hearing, the Court now finds that the government has carried its burden of showing that good cause exists to restrict Sterlingov from reviewing the

sensitive, supplemental heuristic information and that the defense has failed to offer any countervailing justification supporting disclosure.

I.

Under Federal Rule of Criminal Procedure 16(d)(1), "[a]t any time the court may, for good cause, deny, restrict, or defer discovery or inspection, or grant other appropriate relief." Fed. R. Crim. P. 16(d); *see also United States v. Cordova*, 806 F.3d 1085, 1090 (D.C. Cir. 2015); *United States v. Johnson*, 314 F. Supp. 3d 248, 251 (D.D.C. 2018). The government bears the burden of showing good cause and must do so with specificity. *See Johnson*, 314 F. Supp. 3d at 251. Good cause may be based on "the safety of witnesses and others, a particular danger of perjury or witness intimidation, [and] the protection of information vital to national security." *See Cordova*, 806 F.3d at 1090 (alteration in original) (quoting Fed. R. Crim. P. 16, Advisory Committee's Note to 1966 Amendment to Former Subdivision (e)). The Advisory Committee's Notes to the 1966 amendment to Rule 16 also lists, "[a]mong the considerations to be taken into account by the court," "the protection of business enterprises from economic reprisal." Fed. R. Crim. P. 16, Advisory Committee's Note to 1966 Amendment to Former Subdivision (e). "[O]nce a showing of good cause has been made, the court has . . . discretion to fashion an appropriate protective order." *Johnson*, 314 F. Supp. 3d at 251.

Here, good cause exists for limiting access to the sensitive, supplemental heuristic material in the manner that the government proposes. As government counsel persuasively explained at the November 13, 2023 hearing, the material at issue is neither evidence against the defendant nor is it exculpatory evidence. *See* Hrg. Tr. (Rough at 2–3, 16). Instead, the information is best understood as a supplemental expert disclosure. It was provided to the defense, at the Court's urging, to ensure that the defense was fully apprised of the heuristics used

in Chainalysis's Reactor software, which the government's experts, Luke Scholl and Elizabeth Bisbee, used to cluster certain blockchain transactions at issue in the case. This supplemental expert disclosure did not exist at the time either of the government experts prepared their reports, and the government itself came into possession of the material from Chainalysis only as an intermediary, before passing it along to defense counsel. *See, e.g.*, Dkt. 188 at 1.

The government also explained that the sensitive, supplemental heuristic information provides a more granular account of the behavioral heuristics that Reactor employs than the account previously disclosed to Sterlingov, defense counsel, and an array of defense experts in Bisbee's expert report and appendices. That additional detail includes "exactly how" specific behavioral heuristics are "implemented and weighed," and, significantly, it "includes information about the kickouts"—that is, "what behavior would cause Chainalysis *not* to cluster" a given address. Nov. 13, 2023 Hrg. Tr. (Rough at 7–10) (emphasis added). Armed with this information, those bent on preventing the government (or its expert) from clustering addresses, and thereby identifying their owners and connecting them to potentially illicit transactions, could readily adjust their conduct to evade detection. *Id.* at 10.

By way of analogy, consider criminal enterprises that engage in sophisticated bank robberies. Imagine that the government can identify those enterprises by tracking down shell companies that have engaged in certain behaviors—say, opening a new bank account within *x* hours of a robbery and making deposits into that account between one and *y* hours post-robbery and then never again. Imagine further that the government has studied the behavior of particular criminal enterprises and knows that for Enterprise A, "*x*" equals 48 hours and "*y*" equals 12 hours, but that for Enterprise B, "*x*" equals 24 hours and "*y*" equals 6 hours. Armed with details about their behavioral patterns, the government would be able to identify which criminal

enterprise likely robbed a particular bank. And were that information ever to be made public, both Enterprise A and Enterprise B would be able to evade detection by changing their distinctive behaviors. As the government explains it, the defense—including Sterlingov—has long had access to the general methodology that Chainalysis uses. To continue the analogy, they know that the government pays attention to the timing of account openings and deposit patterns. But what the sensitive, supplemental heuristic information discloses is the precise temporal windows—the *x* and *y* values—used for each of the services, and darknet marketplaces, at issue. *See generally id.* at 12–13.

The testimony elicited during the multiple *Daubert* hearings in this case confirm that the sort of cat-and-mouse dynamic described above is far from hypothetical. To take just one example, services like Chainalysis (as well as defense expert, Ciphertrace) rely on the fact that when multiple addresses contribute bitcoin to fund a single transaction, the contributing addresses are likely owned by the same entity. *See* Gov't's Ex. 20 at 6 (Bisbee Expert Report); Aug. 22, 2023 Hrg. Tr. 163 (Still) (testifying that the "co-spend technique is highly reliable and the most-used metric in commercial blockchain analysis tools").[1] That is because, in order to contribute bitcoin to a transaction, an individual must have the private key to the address that originally held the bitcoin in question. *See United States v. Harmon*, 474 F. Supp. 3d 76, 81 (D.D.C. 2020) (explaining that a "sender must sign [a] transaction using a digital signature generated using the sender's private key"). Private keys are like bank account passwords—for

[1] This phenomenon is often referred to as the "co-spend" or "common spend" heuristic, and its origins can be traced back to the white paper on bitcoin authored by its pseudonymous inventor. *See* Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, at 6 (2008), https://bitcoin.org/bitcoin.pdf ("Some linking is still unavoidable with multi-input transactions, *which necessarily reveal that their inputs were owned by the same owner*. The risk is that if the owner of a key is revealed, linking could reveal other transactions that belonged to the same owner." (emphasis added)).

obvious reasons, account owners are unlikely to share them with strangers. *See id.* "Coinjoin" services, however, permit individuals to contribute bitcoin to each other's transactions, without sharing their private key information with one another, thereby defeating (or at least frustrating) the assumption that when multiple addresses fund a single transaction, they are controlled by one entity. *See* Dkt. 149-1 at 3 (Bisbee Decl.). In response to the advent of coinjoin services, law enforcement clustering products like Chainalysis's Reactor and Ciphertrace's Inspector, in turn, have developed (or have attempted to develop) methods of detecting the presence of coinjoin services. *See id.* ("Chainalysis has controls in place to detect CoinJoin and can skip the CoinJoin co-spends so the addresses are not clustered/associated."); Aug. 23, 2023 Hrg. Tr. 245–47 (Still) (testifying that she would need to speak to Ciphertrace's engineering team before confirming how and if Inspector controls for coinjoins).

In this manner, each disclosure of how the government (or its experts) cluster or track bitcoin transactions ups the ante in the detection-evasion, cat-and-mouse game. Indeed, the government alleges that Bitcoin Fog, a bitcoin mixing service, was itself designed and employed to help bitcoin users avoid clustering and tracing of their on-chain activities. Dkt. 1-1 at 1–2 (Crim. Compl.); *see also Matter of Search of Multiple Email Accounts*, 585 F. Supp. 3d 1, 8 (D.D.C. 2022) (explaining that bitcoin mixers or tumblers employ a method "whereby one user's payment or transaction is jumbled with other payments and transactions to make it harder to detect the owner of the [bitcoin]"); *Harmon*, 474 F. Supp. 3d at 82. Against this backdrop, the Court finds that the government's concern regarding providing Sterlingov, the alleged administrator of Bitcoin Fog, with personal access to the granular behavioral heuristics used by Chainalysis is both valid and substantial.

At the November 13, 2023 hearing, the Court inquired whether the granular heuristics in the sensitive, supplemental information remain confidential and in use today, given the speed with which technology develops. *See* Dkt. 210 at 15 ("It is unclear, for example, how the additional detail would make it easier to evade blockchain tracing, how frequently methodologies change (and thus how quickly the information at issue may become outdated) . . . ."). In response, the government assured the Court that these heuristics "are still used for clustering . . . being actively built and tested by Chainalysis now" and that the government is relying on this clustering "in very significant criminal cases and significant national security cases where [the government has] a very important and compelling interest [in] not allow[ing] [the government's] adversaries to . . . contravene those measures." Nov. 13, 2023 Hrg. Tr. (Rough at 10–11). In short, the measures and details at issue are neither inactive nor obsolete.

The Court also inquired whether at least portions of the sensitive, supplemental information might be disclosed without posing a risk to ongoing criminal or national security investigations. In response, government counsel stated:

> Your Honor, we did review in the Court's opinion and order the suggestion that we look at whether there [are] things that may be less sensitive. What we found [is] that really anything that was less sensitive was really in the prior report and if we went through to try and redact out what would be considered active and sensitive, we would essentially . . . be eliminating [from the attachments] the additional columns that were added to this report[,] so it would put [the] defense pretty much back at what the original attachments [to the Bisbee report] were.
>
> And[,] then[,] with the report[] itself, we would—it would look like a series of black boxes without anything really in the way of substantive information that would be of any sort of use to the defendant.

Id. (Rough at 12). Defense counsel, who have had access to the sensitive, supplemental material for several weeks now, did not disagree with this assessment or with the government's more

general representation that disclosure of the information would permit those engaged in illicit bitcoin transactions to evade clustering or tracking.

Rather than take issue with the government's characterization of the sensitive, supplemental information or with the risk that disclosure might undermine ongoing law enforcement and national security activities, the defense argues that the government's request is impermissibly premised on the assumption that Sterlingov is guilty of the crimes with which he is charged (and that, as such, he cannot be trusted to comply with the supplemental protective order, and he has the means and the motive to use the supplemental heuristic information to evade clustering in the future). Dkt. 207 at 2, 7–8. The defense is, of course, correct that every criminal defendant is presumed innocent unless and until the government carries its burden of proof beyond a reasonable doubt. But that does not mean that the Court is required to ignore the government's concerns regarding ongoing criminal and national security investigations. This concept is not novel. Indeed, it is the very premise of the Classified Information Procedures Act ("CIPA"), 18 U.S.C. App. III, §§ 1–16, that, at times, it is appropriate to limit a criminal defendant's access to sensitive information that his or her counsel can review, notwithstanding the presumption of innocence. And, although CIPA deals with uniquely sensitive information, it does not stand alone; to the contrary, it is not unusual for courts to limit access to sensitive information to defense counsel alone, barring access by the defendant himself. *E.g.*, *United States v. Byrd*, 2023 WL 2822154, at *1–2 (S.D.N.Y. Apr. 6, 2023); *United States v. Felix-Aracena*, 2022 WL 17352436, at *1–2 (S.D.N.Y Dec. 1, 2022); *United States v. Lambert*, 2020 WL 6257119, at *1–2 (S.D.N.Y. Oct. 23, 2020); *United States v. Diaz-Rojas*, 2016 WL 4718432, at *2–4 (S.D. Cal. Sept. 8, 2016). Finally, the defense ignores the fact that a grand jury has made a finding of probable cause in this case, which, in other contexts, has been deemed sufficient to

trigger significant, adverse consequences, such as an arrest or temporary loss of employment, *see, e.g.*, *FDIC v. Mallen*, 486 U.S. 230, 241 (1988).

The Court, accordingly, finds (1) that the government has carried its burden of demonstrating good cause for limiting the disclosure of the sensitive, supplemental heuristic information to counsel and qualified experts who are needed to assist counsel and who are prepared to sign a reasonable protective order, and (2) that this good cause extends to the entire sensitive, supplemental production.

II.

The Court must also consider whether Sterlingov's need for access to the sensitive, supplemental information is sufficient to trump the government's showing of good cause for purposes of Rule 16 or, more significantly, whether denying Sterlingov the requested access would violate his rights under the Fifth or Sixth Amendment to the Constitution. The facts of this case do not support his request under either Rule 16 or the Constitution.

In its prior decision, the Court raised the question whether Sterlingov was seeking access to the sensitive, supplemental information so that he could actively assist in his own defense or was merely positing that he, like every other criminal defendant, is entitled to have access to any and all information pertaining to the case against him. Dkt. 210 at 2, 16–17. At the November 13, 2023 hearing, which was held in part so that counsel could answer just this question, *see id.* at 16, Sterlingov's counsel made clear that he was pressing only the latter contention, *see, e.g.*, Nov. 13, 2023 Hrg. Tr. (Rough at 28). Counsel made no mention of any special expertise or knowledge that Sterlingov might bring to bear, *id.* ("We're not attributing any secret skills to [Sterlingov]."), and counsel has failed to take the Court up on its invitation to seek leave, if

necessary, to make any such showing in an *ex parte* submission, *see* Dkt. 210 at 16. More specifically, the following exchange occurred at the November 12, 2023 hearing:

> COURT: That's what I want to drill down on, though. So[,] the point you've just made to me is just as a matter of principle, Mr. Sterlingov should be allowed to examine anything that has a bearing on the accuracy or inaccuracy of the evidence in the case against him. I take that. I will definitely consider that point. Is there anything more than just that sort of [general] notion that as a matter of principle, the defendant in the case ought to have access to anything that might or might not reflect on the accuracy of evidence that's being offered?
>
> COUNSEL: No, Your Honor. That's been our central point. As we said, it's about the Fifth Amendment and the Sixth Amendment issue.
>
> COURT: That's helpful for me to understand. I've been raising these issues about whether there are other individuals that you could have to consult with you. If that's not the argument you're making, that's helpful for me to understand.
>
> COUNSEL: I do want to say that sitting here today, I don't know what—you know, if I am going to use this for impeachment or how I'm going to use it on cross. A lot depends how the direct goes. To the extent that the government is maintaining that it's not important to the defense, we just disagree with that. I think the reasons are obvious.

Nov. 13, 2023 Hrg. Tr. (Rough at 32–33). In short, notwithstanding the Court's observation that, if "Sterlingov is uniquely situated to assist the defense (and thus to ensure that the trial comports with due process)[,] the Court needs to understand why," Dkt. 210 at 16, defense counsel has failed to identify any such justification and, instead, invokes only the general principle that all criminal defendants have the right "to review the evidence against them except[] [in] compelling circumstances," Nov. 13, 2023 Hrg. Tr. (Rough at 21).

Nor can the Court discern any reason why, as a matter of constitutional law, Sterlingov needs access to the highly technical information at issue. As noted above, the information is not evidence that the government intends to offer against Sterlingov, nor did it even exist at the time

Sterlingov was charged. Rather, the information simply provides more granular detail about the behavioral heuristics (referred to by Chainalysis as "Heuristic 2") used by Reactor to cluster and attribute addresses that, according to the government's experts, show that Bitcoin Fog was used to launder large amounts of cryptocurrency associated with certain darknet sites. Notably, moreover, the parties seem to agree that the information at issue has no bearing on the core question of whether Sterlingov operated Bitcoin Fog. Nov. 13, 2023 Hrg. Tr. (Rough at 23–24, 28). And, even with respect to the question of how many transactions (and thus how much money) traveled from addresses affiliated with darknet sites to Bitcoin Fog, and vice versa, the parties seem to agree that many (although not precisely how many) such transactions occurred. *See id.* (Rough at 31–32). As the Court observed at the hearing—without disagreement from the defense—the defense's own expert, Jonelle Still of Ciphertrace, seemed to concede at her *Daubert* hearing that a substantial portion of Bitcoin Fog's activity involved darknet customers.[2] *Id.* The dispute is only about how big a portion that was.

[2] Chainalysis attributed over 900,000 addresses to transactions with Bitcoin Fog and, according to Still, Ciphertrace agrees with respect to almost 400,000 of those addresses. Aug. 22, 2023 Hrg. Tr. 189 (Still). Although the Court will leave this question for the jury, the zone of expert agreement may be even greater than that due to Still's misreading of an appendix provided by Chainalysis that contained a guide for how to parse its data. *Id.* at 185. Moreover, Ciphertrace and Chainalysis's darknet cluster attributions also appear to align with respect to several darknet marketplaces, including Agora (3.5% difference), Sheep (0% difference), Silk Road 2.0 (0% difference), and WelcomeToVideo (1% difference). Dkt. 159-1 at 35 (Still Expert Report). As Still clarified in her testimony at the *Daubert* hearing, the percentage figures in her report are not error rates; rather she used them to quantify how many *more* addresses Chainalysis clustered as compared to Ciphertrace. Aug. 22, 2023 Hrg. Tr. 123–24 (Still). To be sure, the discrepancy rates for other dark market attributions are higher; for example, the discrepancy rate for AlphaBay is 96%, *id.*, but the government explained that the AlphaBay cluster was created in reliance on Heuristic 3, Sept. 7, 2023 Hrg. Tr. 107, which merely refers to information obtained from sources—in the case of AlphaBay "information that was provided by the government following the seizure in that case," *id.*—and thus is unrelated to any on-chain activity or technical process. Indeed, Still testified that, what Chainalysis calls Heuristic 3, Ciphertrace simply calls "direct attribution." Aug. 22, 2023 Hrg. Tr. 150 (Still).

To be sure, it is possible that the magnitude of Bitcoin Fog's transactions with darknet sites might have some bearing on whether the jury believes that the Bitcoin Fog administrator was aware that Bitcoin Fog was being used to launder illicit gains. But the Court has no reason to believe that the more detailed behavioral heuristics described in the sensitive, supplemental information will shed substantially more light on that question than the large quantity of less sensitive expert disclosures already have. Given ample opportunity to show otherwise, the defense simply reverts to *ipse dixit*, asserting: "To the extent the government is maintaining that it's not important to the defense, we just disagree with that" for "reasons [that] are obvious." Nov 13, 2023 Hrg. Tr. (Rough at 33). The Court does not doubt that thorough preparation for trial will include review of this supplemental information, which may (or may not) include detail useful to counsel for cross-examination of the government's experts regarding the magnitude of Bitcoin Fog transactions traceable to the darknet. But, beyond that, the value of the information is far from obvious.

Finally, the Court notes that Sterlingov has long had access to reams of information relating to Chainalysis's efforts to connect hundreds of thousands of darknet bitcoin transactions to Bitcoin Fog. All that is at issue here is the most granular detail regarding the assumptions used in one category of heuristics (Heuristic 2) that Chainalysis employed to draw those connections. It is important that defense counsel (with the assistance of an expert, if necessary) have access to that more detailed information to ensure that no stone is left unturned in preparing Sterlingov's defense. But, as defense counsel conceded after having reviewed the sensitive, supplemental material, he is unsure whether or how he will make use of the information in cross-examining the government's expert, Nov. 13, 2023 Hrg. Tr. (Rough at 33–34), nor has he

identified (at the hearing or in any *ex parte* filing) anything in the supplemental material that Sterlingov himself needs to review in order to assist counsel in preparing the defense.

The Court, accordingly, concludes that Sterlingov has failed to identify any reason why he personally needs to review the sensitive, supplemental information, which might overcome the government's showing of good cause.

CONCLUSION

For the foregoing reasons, the Court finds that good cause exists to restrict defendant Roman Sterlingov from personally reviewing the sensitive, supplemental heuristic information.

SO ORDERED.

/s/ Randolph D. Moss
RANDOLPH D. MOSS
United States District Judge

Date: November 30, 2023