UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	**CRIMINAL NO. 21-cr-399 (RDM)**
	:	
ROMAN STERLINGOV,	:	
	:	
Defendant.	:	

GOVERNMENT'S RESPONSE TO SEPTEMBER 18, 2023 MINUTE ORDER REGARDING DEFENDANT'S ACCESS TO SENSITIVE HEURISTICS INFORMATION PROVIDED BY CHAINALYSIS

The United States of America, by and through the United States Attorney for the District of Columbia, files the following response in response to the Court's minute order on September 18, 2023, directing the government to submit "a brief in support of its position that the protective order at Dkt. [196] restricts Defendant from viewing the materials in question." *See* Minute Order (Sept. 18, 2023). The referenced restriction applies specifically to the highly sensitive, proprietary heuristics information Enhanced Protective Order provided by Chainalysis in September 2023.

LEGAL STANDARD

This Court has broad discretion to fashion an appropriate Protective Order under Fed. R. Crim. P. 16(d)(1), which provides that "[a]t any time the court may, for good cause, deny, restrict, or defer discovery or inspection, or grant other appropriate relief." As the D.C. Circuit has advised, "a 'trial court can and should, where appropriate, place a defendant and his counsel under enforceable orders against unwarranted disclosure of the materials which they may be entitled to inspect.'" *United States v. Cordova*, 806 F.3d 1085, 1090 (D.C. Cir. 2015) (quoting *Alderman v. United States*, 394 U.S. 165, 185 (1969)).

The party seeking the protective order bears the burden of showing "good cause." *Id.* Good cause may be based upon, but is not limited to, "the safety of witnesses and others, a particular danger or perjury or witness intimidation, the protection of information vital to the national security, and the protection of business enterprises from economic reprisals." Fed. R. Crim. P. 16 Advisory Committee's Notes to 1966 Amendment. Courts balance the risk that disclosure would pose a "hazard to others" against any prejudice to the defendant and the public's interest in disclosure. *United States v. Dixon*, 355 F. Supp. 3d 1, 4 (D.D.C. 2019). "[O]nce a showing of good cause has been made, the court has relatively unconstrained discretion to fashion an appropriate protective order." *United States v. Johnson*, 314 F. Supp.3d 248, 251 (D.D.C. 2018); *see also* 2 Charles Alan Wright & Peter J. Henning, Federal Practice & Procedure § 262 (4th ed. 2009) ("The discretion provided to the trial court by Rule 16(d)(1) is vast.").

The defendant does not have a right to personally review all discovery materials. "The Supreme Court has made clear that '[t]here is no general constitutional right to discovery in a criminal case.'" *United States v. Bisong*, 645 F.3d 384, 396 (quoting *United States v. Ruiz,* 536 U.S. 622, 629 (2002)); *see also, e.g.*, *Galloway v. United States*, No. CR RDB-10-775, 2018 WL 1326399, at *3 (D. Md. Mar. 15, 2018) ("Where security is a concern, the right to discovery is not unfettered."). Courts have repeatedly denied claims that a criminal defendant must review every single document produced in discovery. *See, e.g.*, *United States v. Faulkner,* 2011 WL 3962513 at *4 (N.D. Tex. Sept. 8, 2011) (denying continuance to a defendant who wanted "to review all of the data himself and discuss this evidence with his attorney," explaining: "Faulkner cites no authority for his argument that, to be ensured effective assistance of counsel, a defendant must be able to personally review all of the relevant discovery before trial. . . . Faulkner's personal review of the disclosed digital data prior to trial is not constitutionally required or otherwise legally mandated where, as here, Faulkner is represented by counsel who has had the ability to review the discovery before trial."); *United States v. Thompson*, 2013 WL 1809659, at *6–7 (D. Me. Apr. 29, 2013), *aff'd*, 851 F.3d 129 (1st Cir. 2017) ("Thompson does not assert either that the government failed to provide his lawyer with the discovery materials or that his lawyer failed to review discovery, only that Thompson *personally* was not given the opportunity to review the materials. Thompson was not representing himself, such that he needed to assess on his own what evidence was admissible and how persuasive it was. Courts appoint lawyers for defendants in criminal cases so that the lawyers can do the legwork in preparing for trial and give sound advice about whether a defendant should go to trial or plead guilty.").

Consistent with these principles, courts can and do enter protective orders in criminal cases containing "Attorneys' Eyes Only" (AEO) provisions limiting disclosure of certain sensitive materials to defense counsel only. *E.g.*, *United States v. Byrd*, 2023 WL 2822154 (S.D.N.Y. Apr. 6, 2023); *United States v. Felix-Aracena*, 2022 WL 17352436 (S.D.N.Y Dec. 1, 2022); *United States v. Lambert*, 2020 WL 6257119 (S.D.N.Y. Oct. 23, 2020). The decision in *United States v. Diaz-Rojas*, 2016 WL 4718432 (S.D. Cal. Sept. 8, 2016), presents an instructive example. In *Diaz-Rojas*, a Magistrate Judge entered an AEO provision in a drug trafficking case to protect sensitive law enforcement records relating to the training of the drug detection dog that alerted on the defendant's vehicle. *See id.* The court recognized the government's concern that the records, if disclosed, "may be used by criminals, drug trafficking organizations, and terrorists to 'reverse engineer' the training methods and techniques and would reasonably be expected to risk circumvention of the law." *Id.* at *3 (quoting CBP Decl.). Accordingly, the court approved of the AEO designation over these records, finding that the restriction would strike an appropriate balance between the "high risk of harm to the government" and the "de minimis" prejudice to the defendant "given the technical nature of the information and its attenuated pertinence to the elements of the offense for which the defendant is charged." *Id.* at *4.

Courts have also upheld restrictions on defendants' ability to review certain sensitive records in other contexts, including Jencks Act productions, CIPA litigation, and review by defendants in pretrial detention. *E.g.*, *United States v. Hung*, 667 F.2d 1105, 1107-08 (4th Cir. 1981) (affirming protective order restricting defendants from viewing disputed Jencks Act materials, where "the comments of defendants and their further testimony could not have been of any aid in reaching a decision"); *United States v. Fuller*, 2017 WL 3457166, at *3-4 (S.D. Cal. Aug. 11, 2017) (entering protective order with AEO provision for Jencks Act materials relating to cooperating witnesses); *United States v. Mejia*, 448 F.3d 436, 454-59 (D.C. Cir. 2006) (affirming protective order restricting defense review of classified documents); *Bisong*, 645 F.3d at 397 (finding no prejudice where defendant's "retained counsel and AFPD had access to the seized records and discovery materials," even if "arrangements for [the defendant] to have personal access prior to trial did not work out to the full extent ordered by the district court"); *United States v. Youker*, 2015 WL 13864169, at *2 (E.D. Wash. Apr. 30, 2015) (finding that pro se defendant was not entitled to "possession of all discovery materials in pretrial detention," and "[t]his is especially true given the reasonable solution that the Court has provided by appointing standby counsel"). In doing so, courts have reinforced the principle that reasonable restrictions on access to sensitive materials are consistent with defendants' trial and discovery rights.

ARGUMENT

A. Good Cause Exists To Maintain the Protective Order Restrictions

There is good cause to prevent the defendant from personally accessing and reviewing the highly sensitive and proprietary Chainalysis heuristics information at issue. Such a restriction is necessary to prevent inadvertent disclosure of sensitive law enforcement techniques, and to prevent the defendant or others from developing criminal countermeasures to blockchain analysis. *See,* *e.g.*, *United States v. McCaughey*, 534 F. Supp. 3d 132, 139 (D.D.C. 2021) (finding good cause for protective order where disclosure could "reveal the sources and methods law-enforcement officials have used, and will continue to use, to investigate other criminal conduct related to the publicly filed charges"); *Diaz-Rojas*, 2016 WL 4718432, at *3-4 (entering protective order where disclosure might allow criminal adversaries "to 'reverse engineer' the training methods and techniques" at issue). The supplemental Chainalysis heuristics information contains granular, non-public information about the behavioral heuristics used to "fingerprint" specific Darknet markets and other illegal services, as well as information about the techniques used by Chainalysis to detect and control for adversarial coinjoin services intended to obfuscate Bitcoin transactions. As in *McCaughey* and *Diaz-Rojas*, there is a significant risk that disclosure would allow the defendant or others to develop specific countermeasures to these sensitive techniques.

The defendant's primary purpose in operating Bitcoin Fog for nearly a decade was to help customers launder their funds in a way that could not be traced by blockchain analysis firms like Chainalysis, or their law enforcement and financial institution compliance customers. The defense's own expert, Dr. Cabanas, has described an "arms race" with the blockchain analysis companies and the individuals trying to evade their tracing capabilities. 6/6/23 Tr. at 124. This is borne out in the defendant's own statements through his alter-ego, Akemashite Omedetou, describing the various features that Bitcoin Fog was implementing specifically to prevent "the authorities" from doing "statistical analysis" or tracing transactions.

As discussed in prior briefing, *see* ECF No. 61, 73, the defendant has devoted extensive attention and study to attempting to evade "statistical analysis" by blockchain analysis firms and "the authorities." This concern is repeated extensively in the defendant's posts to Bitcoin Talk using the moniker Akemashite Omedetou. For example, in a November 8, 2013, post, Akemashite

Omedetou posted, "I imagine that by now, someone somewhere has sniffed enough information about fog addresses for being able to tell when a transaction goes in or out of the Fog." The post went on to explain the value of Bitcoin Fog's withdrawal waiting periods, noting, "If someone sees two transactions, in and out of the fog, approximately for the same amount at the same time, there the connection can be made as well." In another post, Akemashite Omedetou cautioned users that they should "never withdraw the same amount as you have deposited" from Bitcoin Fog. As the defendant explained, "If you transfer 1.382 to us, and the next day you withdraw ~1.38 bitcoins to another account, those amounts will be visible in the block chain, and unless there were 10 other people that day that also withdrew just 1.38 bitcoins, the link between your deposit and your withdrawal will be pretty obvious."

On June 30, 2012, Akemashite Omedetou announced that Bitcoin Fog would begin reusing deposit addresses in order to enhance customer anonymity. Akemashite Omedetou explained: "This seems to help obscuring the origin of the bitcoins: even if authorities would find one of your deposit addresses, they won't even be sure that all the deposits to that address were made by you." This is a reference to attempting to prevent law enforcement authorities from using blockchain analysis to trace deposits into Bitcoin Fog and attribute them to a particular user.

The defendant operated a service that was designed to circumvent what the defendant understood to be the "authorities" ability to conduct blockchain analysis. Providing the defendant a highly detailed breakdown of the heuristics used by Chainalysis to cluster Bitcoin Fog and other darknet services would be handing him a roadmap to circumvent this analysis in the future. As the defense's own expert Ms. Still conceded, criminals use mixing services to conceal their illicit activity. *See* 8/22/23 Tr. at 171. Additionally, some illicit actors use CoinJoin implementations in order to evade tracing and attribution by blockchain analysis firms. Revealing the heuristics used to detect and cluster mixers, and the techniques used to control for CoinJoin, would jeopardize numerous law enforcement investigations and impact the effectiveness of law enforcement tracing tools. This supports a finding of good cause to restrict the defendant's access to the materials.

B. The Defendant Is Not Prejudiced by the Protective Order

At the outset, it is important to recognize the *sui generis* nature of the Chainalysis heuristics information at issue here. The heuristics information is not evidence that the government will introduce against the defendant at trial. The heuristics information did not even exist, and it was certainly not in the prosecution team's possession, before Chainalysis compiled it for purposes of this litigation—and thus it falls outside the scope of ordinary criminal discovery under Rule 16(a)(1)(E), let alone *Brady* or *Giglio*. The heuristics information was not consulted or relied upon by any of the government's experts in forming their opinions—and thus it falls outside the scope of expert disclosure and discovery under Rule 16(a)(1)(G). Instead, the heuristics information was compiled and voluntarily disclosed by Chainalysis to the defense, prompted by an overbroad Rule 17(c) subpoena, for the sole purpose of assisting the defense expert and defense team in vigorously cross-examining the government's blockchain experts. Under such unique circumstances, the government is unaware of *any* legal authority supporting any claimed "right" by the defendant to personally review the sensitive heuristics information. *See Mejia*, 448 F.3d at 458 (finding no Fifth or Sixth Amendment right by defendant *or even defense counsel* to review classified material that did not qualify as *Brady*).

Further, there is no prejudice to the defendant in precluding him from personally reviewing Chainalysis' sensitive, proprietary heuristics information. While it is true that a protective order may not be so restrictive as to deny "an accused's constitutional right to the effective assistance of counsel in criminal prosecutions," *United States v. Torres*, 2020 WL 4500046, at *4 (D.N.J. Aug.

5, 2020), the defendant has been and will continue to be a full partner in assisting his attorneys even without the additional, highly technical information provided in the supplemental heuristics information. *See id.* at *6 (finding no prejudice from protective order which provided "a reasonable layer of security for the victims without unduly burdening or hampering Defendant's counsel"). The defendant has been able to review prior discovery productions, consistent with the terms of the Protective Order in this case, read the government's expert reports, and participate in extensive *Daubert* hearings regarding clustering and blockchain analysis. Indeed, the defendant has competent and zealous defense counsel who will be reviewing the materials to hone their cross-examination of the government's blockchain experts and to inform their arguments about the efficacy of the Chainalysis heuristics.

Here, as in *Diaz-Rojas*, the "technical nature of the information" further weighs against the defendant's need for personal access. 2016 WL 4718432, at *4. The defendant has never before seen the sensitive heuristics information at issue and can offer no personal insight or contextual information about it to his attorneys —unlike virtually all of the other evidence in this case, such as the defendant's email communications, or translations of the defendant's handwritten or electronic notes, or even records of the defendant's personal transactions on Mt. Gox and other cryptocurrency platforms. The defendant is presumably not intending to take the stand to testify about his own expert assessment of the heuristics—as doing so would be tantamount to a concession that he did, in fact, operate Bitcoin Fog and thus does have an expert-level knowledge of clustering heuristics. There is no prejudice to the defendant in limiting his personal review of this narrow, highly technical sliver of the massive volume of discovery in this case.

CONCLUSION

Good cause exists to restrict the defendant from reviewing the sensitive Chainalysis heuristics information. The defendant is not prejudiced by not being permitted to review the materials himself.

Respectfully submitted,

MATTHEW M. GRAVES
UNITED STATES ATTORNEY
D.C. Bar No. 481052

BY: *_/s/ Christopher B. Brown_*
Christopher B. Brown, D.C. Bar No. 1008763
Assistant United States Attorney
U.S. Attorney's Office for the District of Columbia
601 D Street, N.W.
Washington, D.C. 20530
(202) 252-7153
Christopher.Brown6@usdoj.gov

*_/s/ C. Alden Pelker_*
*_/s/ Jeffrey Pearlman_*
C. Alden Pelker, Maryland Bar
Jeff Pearlman, D.C. Bar No. 466901
Trial Attorneys, U.S. Department of Justice
Computer Crime & Intellectual Property Section
1301 New York Ave., N.W., Suite 600
Washington, D.C. 20005
(202) 616-5007 (Pelker)
(202) 579-6543 (Pearlman)
Catherine.Pelker@usdoj.gov
Jeffrey.Pearlman2@usdoj.gov