PDFs mentioned [redacted]). Lawyer B explained that "on the off [chance] that someone would try to assert that [the PDFs] were [Subject 1's] documents[,] out of prudence, [redacted] took the extra step to . . . redact or remove any information that could arguably be subject to a claim of privilege." Hr'g Tr. at 31:23–32:2. This interaction with the OSC was the Subjects' first contact with the government regarding the hacking incident. *See id.* at 31:1–32:9; Subjects' Mem. at 5.

Meanwhile, Lawyer A represented the Subjects [redacted] in various matters in California and, in this capacity, reported the hacking incident, on March 22, 2018, to the California U.S. Attorney's Office ("California USAO"), prompting the office to open an official investigation. Lawyer A Decl. ¶ 14. Subsequently, Law Firm A "communicated regularly and extensively with the [California] USAO and FBI in the spring of 2018" through in-person meetings as well as via telephone and email. *Id.* ¶¶ 15–16. The FBI also interviewed both Subjects. *Id.* ¶ 16.

As part of the California USAO and FBI's investigation of the hacking incident, "the government continually requested evidence and information from the [Subjects], which the government emphasized would be essential to identifying the perpetrators and to detecting and mitigating the cybersecurity threat." *Id.* ¶ 17. Lawyer A states that the Subjects provided information to law enforcement to assist in the identification of the perpetrators, and that Law Firm A "on multiple occasions explained to the [California] USAO and FBI that materials from the [Subjects] that cyberattackers had accessed and stolen were confidential and highly sensitive." *Id.* ¶ 18. Consequently, Law Firm A declined requests from the FBI and California USAO for access to [redacted]s servers and email accounts, *id.*, or for the FBI to collect forensic evidence from the Subjects' computer systems on the grounds that "doing so would

disclose confidential and sensitive communications, including many privileged communications," *id.* ¶¶ 19–20.

In April 2018, the California USAO and FBI requested "copies of the leaked PDF documents" that had been disseminated to the media, *id.*, Ex. G, Emails Between Lawyer A and FBI (Apr. 2018), at 100, ECF No. 16–2; *id.* ¶¶ 21–22, 30, in order "to obtain original, forensic evidence of the cyberattacks and identify the methods employed by the cyberattackers," *id.* ¶ 23, using "those files [that] originated from the cyberattackers who created them, . . . because [Law Firm A's] investigation had uncovered metadata information in the [files] that would be important to identify and stop the cyberattackers and those involved," *id.* Law Firm A was "particularly mindful that any alterations to these documents risked destroying important forensic data." *Id. See also* Subjects' Reply Mem. in Supp. of Mot. for Reconsideration ("Subjects' Reply") at 1, ECF No. 28 ("For the documents to be useful to the government, the [Subjects] had to provide them in the same form in which they themselves had received them from media sources (who had, in turn, apparently received them from third parties who had compiled and, in some cases, altered ostensible reproductions of the [Subjects'] stolen documents.")).

Law Firm A provided the FBI with a total of 45 PDFs "which [Law Firm A] did not alter in any manner so as to preserve all the original forensic evidence . . . and to avoid introducing forensic 'junk' into these files." *Id.* ¶ 31. While aware that these Disclosed PDFs contained "purported copies of private, confidential, and/or privileged communications between and among" the Subjects, *id.* ¶ 14, Lawyer A avers that "at no time" did he or Law Firm A represent "that the [Disclosed PDFs] constituted or reflected authentic records that were kept in the normal course of business," *id.* ¶ 32; *see also id.* ¶ 28. Instead, Lawyer A says that he "explained that it

was possible that some of the emails were fake" and that "it was not possible to determine if documents were authentic." *Id.* ¶ 32. Thus, to the best of the Subjects' knowledge, the government does not have a "basis for assuming or asserting that the [documents] constituted or reflected authentic records that were kept in the normal course of business by the [Subjects]." *Id.*; [redacted] Lawyer A further stresses that in providing the Disclosed PDFs to the FBI, the Subjects "did not intend to waive any privilege attaching to the communications ostensibly reflected therein, nor did they intend to waive any privilege attaching to the confidential records that were kept in the ordinary course of business by" [redacted] or the Subjects. Lawyer A Decl. ¶ 33. In fact, Law Firm A "sought to protect the confidentiality of the [Disclosed PDFs]" by transferring them via "a secure [File Transfer Protocol ("FTP")] designed to ensure the security and confidentiality of the transmitted information." *Id.* ¶ 34. Lawyer A implies that law enforcement officials, not Law Firm A, were responsible for any privilege waiver, complaining that "[a]t no point did the [California] USAO or FBI inform [Law Firm A] or the [Subjects] that privileged information may have been inadvertently produced to the government, or that the information provided by [Law Firm A] would be disseminated beyond the named recipients." *Id.* ¶ 36; *see also id.* ¶ 46.

On June 8, 2018, the California USAO informed Law Firm A that the criminal investigation would be stayed, *id.* ¶ 50, and the Subjects shared no additional information with the California USAO or the FBI after this point, *id.* ¶ 51. On October 3, 2018, the California USAO informed the Subjects of its decision not to proceed further with a criminal investigation. *Id.* ¶ 52.

The Subjects indicate that, of the 45 Disclosed PDFs, (1) four appear to have been entirely fabricated by unknown third parties; (2) [redacted] containing altered versions of emails and other communications; and (3) "several" contain stolen communications that have been altered and presented to appear to be related, despite the fact that the authentic communications upon which they are based are unrelated in time and/or subject matter. Lawyer B Decl. ¶ 9. Other than describing the 34 pages of potentially privileged emails between or among the Subjects and their counsel as appearing in multiple Disclosed PDFs, *see* H'rg Tr. at 24:16–24; *id.* at 47:14–24, the Subjects have not clarified whether these 34 pages appear only in the six PDFs identified by the Subjects as fabricated by unknown parties [redacted] or in the "several" PDFs containing some altered emails. *Id.* at 24:16–25:2 (Subjects' counsel stating that 34 pages were "broadly scattered around [those documents]" and "I will get you the exact number" of the Disclosed PDFs containing the 34 pages).[9]

C. Investigative Steps Subsequent to the 2018 Decision and Negotiations to Encourage Subjects' Compliance with Subpoenas

Following the 2018 Decision, on July 9, 2018, law enforcement agents executed search warrants on Subject 1's business and the Subjects' [redacted] in California. Gov't's Opp'n at 6. That same day, the Subjects were served with grand jury subpoenas for an investigation of possible violations of federal criminal laws, including "[redacted], conspiracy to act as an unregistered foreign agent, c[redacted] [those] statutes, [18 U.S.C. §§ 371, [redacted] and 22 U.S.C. §§ 611–21]." Grand Jury Subpoenas, at

[9] The purpose of the Subjects' strategic obfuscation appears intended to leave the government (and the Court) guessing whether the 34 pages are authentic or fabricated/altered emails, and to leave them room simultaneously to disavow the Disclosed PDFs as fake while asserting privilege vigorously over the same contents.

62, 67; *see also* Gov't's Opp'n at 6. With respect to the grand jury subpoenas, the government directed the Subjects to produce non-privileged documents that were outside the scope of the warrants but within the scope of the subpoenas. Gov't's Opp'n at 6. Subject 2 has produced no records in response to the subpoenas, and Subject 1 continues to produce responsive, non-privileged documents. *Id.*; H'rg Tr. at 60:12–61:7.

The following month, in August 2018, the government executed a search warrant on an e-discovery and forensic consulting vendor engaged by Subject 1, seizing "forensic images and copies of numerous digital devices, email servers, and email accounts belonging to [redacted] and [the Subjects]." Gov't's Opp'n at 6; Subjects' Mem. at 9.[10]

Following the execution of the search warrants, the government engaged in extensive discussions with the Subjects' counsel, Lawyer B, to facilitate compliance with the grand jury subpoenas. In connection with these discussions, the government obtained court authorization to disclose the 2018 Order to the Subjects, *see* Order (Aug. 15, 2018), ECF No. 13, which order was provided to the Subjects on August 27, 2018, *see* Gov't's Opp'n at 6; Subjects' Mem. at 1 n.2, and then to disclose a redacted version of the 2018 Decision, *see* Order (Oct. 22, 2018), which redacted decision was provided to the Subjects on October 25, 2018, *see* Subjects' Mem. at 1; Lawyer B Decl. ¶ 15.[11]

Almost two months later, on December 21, 2018, the Subjects filed the instant motion, which was fully briefed over the following three months in accordance with the schedule agreed to by the parties. *See* Min. Order (Dec. 27, 2018). Upon review of the voluminous briefing and

---

10 The consulting vendor is [redacted]. *See* Subjects' Mem. at 9.

11 The government sought partial unsealing of the 2018 Decision as to two categories of factual information: (1) information related to subject matters that would be publicly disclosed through the filing of a civil forfeiture complaint and through the guilty plea of another individual; and (2) information already known to Subjects due to their previous interactions with the FBI. Gov't's Opp'n at 7. The Subjects correctly observe that the "redactions obscured almost entirely the Court's basis for its crime-fraud ruling but revealed the majority of the Court's basis for its waiver ruling." Subjects' Mem. at 1–2.

exhibits, totaling over 600 pages, submitted in connection with the pending motion and the hearing held on April 2, 2019, the Subjects' motion is now ripe for resolution.

II. STANDARD OF REVIEW

The parties do not address the standard of review applicable to the unusual procedural posture of the Subjects' request for review, pre-indictment, of the government's judicially sanctioned access to otherwise privileged material in the Disclosed PDFs. Federal Rule of Criminal Procedure 12(b)(3) requires that certain pretrial motions be raised "if the basis for the motion is then reasonably available and the motion can be determined without a trial on the merits," including for "suppression of evidence," FED. R. CRIM. P. 12(b)(3)(C), but appears to contemplate that a criminal proceeding is pending, which is not the situation here. *See* FED. R. CRIM. P. 12(b)(1) (noting that, "[i]n [g]eneral," a "*party* may raise by pretrial motion . . .") (emphasis added). Although providing scant guidance, case law suggests that pre-indictment review is only available in unique circumstances. *See United States v. Search of Law Office*, 341 F.3d 404, 409, 414 (5th Cir. 2003) (holding that courts have a "unique power" to order suppression or return of unlawfully seized property prior to return of an indictment, but that "such jurisdiction should be exercised with caution and restraint, and subject to equitable principles," requiring "at the very least, a substantial showing of irreparable harm"); *see In re Berkley & Co. Inc.*, 629 F.2d 548, 550 (8th Cir. 1980) (discussing a prior remand to the district court to reconsider its pre-indictment privilege decision *de novo* in light of additional documents not previously available to it).

Although the precise standard for review of the Subjects' reconsideration motion is neither clear nor elucidated by the parties, the subject matter waiver ruling is reviewed *de novo,* informed by the Subjects' recitation of the events leading to the Disclosed PDFs' provision to the FBI. *See* H'rg Tr. at 13:14–17:7 (Subjects' counsel arguing for a *de novo* standard of review);

id. at 40:6–25 (government counsel agreeing that the standard of review should be *de novo*). Further, as in analogous, pre-indictment circumstances, where "the party claiming [attorney-client] privilege bears the burden of proving that the communications are protected," *In re Lindsey*, 158 F.3d 1263, 1270 (D.C. Cir. 1998), the Subjects bear the burden of establishing that their asserted privileges persist. *See In re Grand Jury Investigation*, 974 F.2d 1068, 1070 (9th Cir. 1992) (in grand jury investigation context, "[t]he party asserting the attorney-client privilege has the burden of proving that the privilege applies to a given set of documents or communications"); *see also Search of Law Office*, 341 F.3d at 413–14 (holding that a movant's pre-indictment Federal Rule of Criminal Procedure 41(g) motion offered merely "vague allegations that the government viewed extensive amounts of privileged information" and failed to offer proof substantiating his assertions).

III. DISCUSSION

The Subjects challenge the 2018 Decision's waiver ruling on a number of grounds and seek access to the reasoning and materials underlying the crime-fraud ruling in order to challenge that part of the decision more fully. Predicated on the Subjects' view that both the waiver and crime-fraud ruling are not sound, they also seek to quash the subpoenas issued against them and a protective order sealing "all documents and materials the government has obtained that contain or purport to reflect the [Subjects'] privileged materials until after [Subjects] have had a full and fair opportunity to persuade the Court to reconsider its *ex parte* crime-fraud ruling," Subjects' Mem. at 3, as well as "prohibiting the government from further accessing or using their privileged materials or information . . . pending a fully contested hearing," *id.* at 23. The Subjects' arguments are examined below.

A. No Subject Matter Waiver From Disclosed PDFs

The Subjects characterize the 2018 Decision's waiver holding as "erroneous as a matter of law." *Id.* at 2. The Subjects' position as to why the waiver holding is erroneous has evolved over the course of the briefing and hearing in this matter. The Subjects initially insisted that the Disclosed PDFs remain privileged, arguing that: (1) theft by a third party does not operate as a waiver, Subjects' Mem. at 16–17; and (2) the Subjects deserve the protections of both the Cybersecurity Information Sharing Act of 2015, 6 U.S.C. §§ 1501–1510 and the Crime Victims' Rights Act, 18 U.S.C. § 3771(a)(8), *see* Subjects' Mem. at 18–20, 25–26; Subjects' Reply at 9–13. At the same time, the Subjects disavowed that any privilege even attached to the Disclosed PDFs since the Disclosed PDFs were created by third parties and did not represent the Subjects' authentic documents. Subjects' Mem. at 13–15.

Perhaps recognizing that the record posed significant obstacles for each of these arguments, the Subjects pivoted at the hearing, and now disclaim any privilege in the Disclosed PDFs, merely seeking reconsideration of the *scope* of the waiver ruling. *See* H'rg Tr. at 18:2–13 (Subjects' counsel clarifying that "[w]hat we care about is the finding of subject matter waiver. . . . [i]f . . . the Court says: As to the [Disclosed PDFs], whatever privilege there is is waived, I have no objection. I don't believe there is a privilege as to them anyway. They are stolen documents that you can get off Google right now today. . . . [w]e can't assert privilege over those, and we don't. What I care about are the thousands and thousands of other documents that this ruling says has no privilege when, in fact, we didn't produce them to the Government intentionally"); *id.* at 30:2–13 (Subjects' counsel reiterating "we are not primarily concerned with these documents. Any human being can go get these documents off of Google. . . . [w]hat I am concerned with are all of the privileged documents that [Lawyer A] acted appropriately to on [April 4, 2018] and said: No, there are lots of privileged documents here; we are not giving them

to you. There [are] no circumstances under which we should be found under those facts to have waived the subject matter of this issue; I think that's the key point.").

At the hearing, the government expressed surprise that the focus of the Subjects' reconsideration motion had shifted to the scope of the subject matter waiver, rather than the privileged status of the Disclosed PDFs. *See* H'rg Tr. at 56:5–8 ("[T]his is, essentially, the first time that the Government has heard [the Subjects'] claim that this is all about the subject matter waiver that would apply to other documents."). Understandably so, given what the government rightly characterizes as the "scattershot" nature of the Subjects' arguments. Gov't's Opp'n at 17. Indeed, although the Subjects briefly mention subject matter waiver in their motion, they made no mention of Federal Rule of Evidence 502, concerning waiver, until their reply. *See* Subjects' Mem. at 13; Subjects' Reply at 3–7. Even then, the Subjects insisted that any waiver was inadvertent, citing only to Federal Rule of Evidence 502(b). *See* Subjects' Reply at 3–7. The true aim of the Subjects' motion—or at least their most viable argument—did not fully come into focus until the hearing. In the context of this ongoing, time-sensitive grand jury investigation, the Subjects' determination to preserve any possible argument has obscured rather than bolstered their claim to relief and hindered rather than aided resolution of their motion.

Now that the Subjects disclaim any privilege in the PDFs, only their subject matter waiver argument merits attention. The Subjects claim that any intentional disclosure and concomitant waiver as to the Disclosed PDFs does not constitute a subject matter waiver under Federal Rule of Evidence 502(a) because: (1) the Subjects continuously warned the FBI that privileged communications were involved and took steps to maintain that privilege, such as refusing to provide undisclosed versions of their communications; (2) removal or redaction of any privileged information in the Disclosed PDFs was not possible without jeopardizing the

forensic evidence related to the cyberattack or otherwise corrupting the files, particularly in light of representations from the FBI that original documents were necessary to investigate the cyberattack against them; and (3) alleged government misconduct demonstrates that the government has taken unfair advantage of the Subjects in order to gain access to privileged material.

The Subjects' insinuations of government misconduct are unsupported by the record since the government has scrupulously protected the Subjects' privileged communications and appropriately sought judicial guidance and authority to access that material. Upon reconsideration, however, the Court concludes that the Subjects' voluntary disclosure of the Disclosed PDFs, while an intentional waiver as to any privileged material contained in those PDFs, did not operate as a waiver, under Rule 502(a), with respect to other, undisclosed privileged communications on the same subject matter. This narrowed waiver ruling has limited impact since the 2018 Decision's crime-fraud ruling remains intact and vitiates the Subjects' and any co-conspirators' privileges with respect to undisclosed communications, obtained through means other than disclosure of the Disclosed PDFs, among the Subjects and/or those co-conspirators to the extent those communications furthered the [redacted] schemes, in violation of 18 U.S.C. §§ 371, [redacted] and 22 U.S.C. §§ 611–21, for which the government had sustained its *prima facie* burden in the *ex parte* application. *See* H'rg Tr. at 58:8–18 (government counsel agreeing that "the bulk of the subject matter at issue here is covered by the crime-fraud exception . . . . [but] a sliver of material . . . would fall outside of the crime-fraud ruling [and] would still be subject to the attorney-client [redacted] waiver and to subject matter waiver related to" the disclosure of the Disclosed PDFs).

1. Privilege Principles

The legal principles underlying waiver of the attorney-client privilege are set out in the 2018 Decision, *see* 2018 Decision at 18–23, and will be only briefly summarized here.

The attorney-client privilege may be waived when the client discloses communications with his or her attorney to a third party and, further, such voluntary disclosure of otherwise privileged communications to one third party amounts to waiver as to all such communications on the subject matter disclosed. *See, e.g.*, *Williams & Connolly v. SEC*, 662 F.3d 1240, 1244 (D.C. Cir. 2011); *United States v. Williams Cos., Inc.*, 562 F.3d 387, 394 (D.C. Cir. 2009); *In re Sealed Case*, 29 F.3d 715, 719 (D.C. Cir. 1994); *In re Sealed Case*, 877 F.2d 976, 980–81 (D.C. Cir. 1989); *Permian Corp. v. United States*, 665 F.2d 1214, 1219 (D.C. Cir. 1981). The D.C. Circuit "adheres to a strict rule on waiver of [the] privilege[]," requiring a privilege holder to "zealously protect the privileged materials" and "tak[e] all reasonable steps to prevent their disclosure." *SEC v. Lavin*, 111 F.3d 921, 929 (D.C. Cir. 1997) (citing *In re Sealed Case*, 877 F.2d at 980).

Adoption in 2008 of Federal Rule of Evidence 502 "modified this Circuit's previously strict rule on subject matter waiver." *Hughes v. Abell*, No. 09-0220 (JDB), 2012 WL 13054819, at *5 (D.D.C. Mar. 7, 2012). Specifically, Rule 502(a) directs that waiver of the attorney-client privilege by intentionally disclosing a privileged communication "in a federal proceeding or to a federal office or agency" serves as a subject matter waiver as to other undisclosed communications or information only if: "(1) the waiver is intentional; (2) the disclosed and undisclosed communications or information concern the same subject matter; and (3) they ought in fairness to be considered together." FED. R. EVID. 502(a). Thus, "Rule 502 does not change the important premise that the disclosure of one communication waives the privilege with respect to other communications concerning the same subject matter when 'they ought in fairness be

considered together,' FED. R. EVID. 502(a)(3), 'in order to prevent a selective and misleading presentation of evidence to the disadvantage of the adversary,' FED. R. EVID. 502 explanatory note." *Hughes*, 2012 WL 13054819, at *5. By contrast, "an inadvertent disclosure of [privileged] information can never result in a subject matter waiver," FED. R. EVID. 502 explanatory note, and does not even result in a waiver as to the disclosed information if the privilege holder "took reasonable steps to prevent disclosure" and "promptly took reasonable steps to rectify the error." FED. R. EVID. 502(b). Rule 502(b) was intended to "reject[]" precedent in the D.C. Circuit holding that "inadvertent disclosure of documents during discovery automatically constituted a subject matter waiver." FED. R. EVID. 502 explanatory note (stating that "[t]he rule rejects the result in *In re Sealed Case*, 877 F.2d 976 (D.C. Cir. 1989), which held that inadvertent disclosure of documents during discovery automatically constituted a subject matter waiver"); *see also Williams v. District of Columbia*, 806 F. Supp. 2d 44, 48 (D.D.C. 2011) (observing that "[i]n this Circuit, it used to be the case that virtually any disclosure of a communication protected by the attorney-client privilege, even if inadvertent, worked a waiver of the privilege" and explaining that "Congress partially abrogated this relatively strict approach to waiver by enacting Rule 502(b) of the Federal Rules of Evidence").

2. Analysis

As the Subjects now recognize, their most—and only—viable argument for reconsideration of the waiver ruling is whether the Subjects' disclosure of the Disclosed PDFs constituted a subject matter waiver as to undisclosed emails on the same topics under Rule 502(a). Nevertheless, in light of the Subjects' vacillations, some discussion of why the Disclosed PDFs are no longer privileged is warranted.

a. The Subjects Intentionally Waived Privilege Over the Disclosed PDFs by Voluntarily Disclosing Them to the FBI

As noted, Rule 502(a) instructs that when a disclosure is made to a federal office or agency and that disclosure waives attorney-client privilege, the waiver only extends to an undisclosed communication if: (1) the waiver was intentional; (2) the disclosed and undisclosed communications or information concern the same subject matter; and (3) they ought in fairness to be considered together. FED. R. EVID. 502(a).[12] This rule does not alter well-settled law that intentional disclosure of a privileged communication generally results in a waiver of the privilege. *Id.* explanatory note ("[T]he rule does not purport to supplant applicable waiver doctrine generally."); *see also In re Subpoenas Duces Tecum*, 738 F.2d 1367, 1369 (D.C. Cir. 1984) ("As stated by this court in *Permian Corp. v. United States*, 665 F.2d 1214, 1219 (D.C. Cir. 1981) (quoting *United States v. American Telephone & Telegraph*, 642 F.2d 1285, 1299 (D.C. Cir. 1980)), 'any voluntary disclosure by the holder of such a privilege is inconsistent with the confidential relationship and thus waives the privilege.'" (alteration omitted) (citing *generally* 8 J. Wigmore, Evidence §§ 2327–28 (McNaughton rev. 1961); McCormack on Evidence § 93 (Cleary ed. 1972)). Here, the Subjects' provision of the Disclosed PDFs to the FBI constituted an intentional waiver under Rule 502(a)(1) of any privilege attached to communications or information of the contents of those electronic files.

To avoid this well-settled legal principle, the Subjects initially raised several arguments insisting that they retained privilege over those communications. None of those arguments has

---

[12] The federal rules of privilege apply to grand jury proceedings, even though other evidentiary rules do not. *See* FED. R. EVID. 1101(d)(2); *In re Grand Jury Subpoena*, 909 F.3d 26, 29 (4th Cir. 2018) ("While the federal rules of evidence generally do not apply to grand jury proceedings, an exception exists for privilege rules."); *In re Grand Jury 16-3817 (16-4)*, 740 F. App'x 243, 244–46 (4th Cir. 2018) (considering, in a grand jury context, the application of a Rule 502(e) agreement preserving privilege); *In re Impounded*, 241 F.3d 308, 313 n.3 (3d Cir. 2001) ("[Federal Rule of Evidence] 1101(d)(2) provides that the rules on privileges articulated by [Federal Rule of Evidence] 501 are applicable to grand jury proceedings.").

merit. First, they contended that any waiver must be classified as inadvertent and analyzed under FED. R. EVID. 502(b). *See* Subjects' Mem. at 14; Subjects' Reply at 5–6. This argument is belied by the record since "disclosure to the FBI was initiated, authorized, and executed by the privilege holders themselves." Gov't's Opp'n at 8. The Subjects rightly abandoned this argument by now clarifying that they only challenge the subject matter waiver ruling and are therefore proceeding under Rule 502(a).[13]

Second, although the Subjects correctly observe that a privilege-holder who takes proper precautions to ensure the confidentiality of her communications is not held to have waived attorney-client privilege when those communications are stolen, *see* Subjects' Mem. at 16–17 (citing, *e.g.*, *Dukes v. Wal-Mart Stores, Inc.*, No. 01-CV-2252 CRB (JSC), 2013 WL 1282892, at *4–6 (N.D. Cal. Mar. 26, 2013) (citing *In re Dayco Corp. Derivative Sec. Litig.*, 102 F.R.D. 468, 470 (S.D. Ohio 1984))), a privilege-holder who intentionally discloses confidential information *in response* to the theft of her confidential materials, as the Subjects did here, may be held to have waived the privilege.[14] In the course of disclosing the Disclosed PDFs to the FBI, the Subjects' counsel conceded that at least some of the PDFs included "legitimate emails." *See*

---

[13] The Subjects' attempt to shoehorn their delivery of the Disclosed PDFs to the FBI into the inadvertent waiver prong of Federal Rule of Evidence 502(b) was strained at best, and thoroughly undermined by their counsel's declarations concerning the disclosure. By his own account, the Subjects' Lawyer A engaged in extensive discussions about materials that would not be disclosed to the FBI on account of privilege concerns, *see, e.g.*, Lawyer A Decl. ¶¶ 18–20, 26–27, but he nevertheless handed over the Disclosed PDFs to the FBI. He was certainly in the best position to understand which of the Disclosed PDFs contained privileged material. *See* Subjects' Mem. at 20 (conceding that "the proponent[s] of the privilege. . . . [are] the 'one[s] with superior access to the evidence and in the best position to explain things.'" (quoting *Matter of Feldberg*, 862 F.2d 622, 625–26 (7th Cir. 1988))). At the hearing, the Subjects wisely pivoted from arguments based on Federal Rule of Evidence 502(b) to arguments based on Federal Rule of Evidence 502(a). *See* H'rg Tr. at 17:8–15, 18:16–22, 29:17–30:1, 30:15–19, 64:5–65:6.

[14] The *Dukes* case, relied upon by the Subjects, illustrates precisely this point. In *Dukes*, a confidential memo related to ongoing litigation was leaked to the *New York Times*, which reported on some of the document's findings but did not publish the actual memo. 2013 WL 1282892, at *1–2. The *Dukes* plaintiff argued that the defendant affirmatively waived privilege by offering a public response to the *New York Times* article. 2013 WL 1282892, at *6. The *Dukes* Court held that while generic responses to the article did not waive privilege as to the entire memo, the defendant's counsel's statement to the *New York Times* disclosing contents of the privileged memo that had not already been published waived the privilege as to that disclosed information. *Id.* at *7–8.

May 18, 2018 FBI 302, at 3. Accordingly, although the initial hacking and dissemination of the Subjects' emails did not waive the Subjects' privilege, the Subjects' voluntary disclosure, through Lawyer A, of the Disclosed PDFs to the FBI was a separate, voluntary waiver as to whatever privilege existed in those Disclosed PDFs.

Third, the Subjects claim the protection of the Cybersecurity Information Sharing Act of 2015 ("CISA"), 6 U.S.C. §§ 1501–1510, which provides that sharing "cyber threat indicators" with the federal government does not operate as a waiver of privilege. *See* 6 U.S.C. § 1504(d)(1); Subjects' Mem. at 18–20.[15] Yet, protection of privilege is not automatic under CISA. Instead, CISA "requires a non-federal entity to remove any information from a cyber threat indicator or defensive measure that it knows at the time of sharing to be personal information of a specific individual . . . that is not directly related to a cybersecurity threat before sharing that cyber threat indicator or defensive measure with a federal entity." Dep't of Homeland Security & Dep't of Justice, Guidance to Assist Non-Federal Entities to Share Cyber Threat Indicators and Defensive Measures with Federal Entities Under the Cybersecurity Information Sharing Act of 2015, 8 (June 2016); *see also* 6 U.S.C. § 1503(d)(2)(A).

In other words, CISA is not an open invitation to share all documents or information connected in any way to a cybersecurity breach without regard to risk of privilege waiver. Here, the Subjects took no steps to remove personal information that was not directly related to the cyberattack prior to sharing the Disclosed PDFs. *See* Gov't's Opp'n at 11 ("[G]iven that the . . .

---

15 CISA defines a "cyber threat indicator" as "information that is necessary to describe or identify," *inter alia*, "malicious reconnaissance," "a security vulnerability," "the actual or potential harm caused by an incident, including a description of the information exfiltrated as a result of a particular cybersecurity threat," "any other attribute of a cybersecurity threat," or "any combination [of such information]." 6 U.S.C. § 1501(6). The Subjects assert that the Disclosed PDFs meet CISA's definition of a cyber threat indicator, Subjects' Mem. at 18–19, and the government does not argue otherwise, Gov't's Opp'n at 10–11. The government maintains, however, that regardless of whether the Disclosed PDFs qualify as "cyber threat indicators," the Subjects failed to comply with CISA's requirement that they conduct a mandatory review for and removal of personal information prior to sharing the Disclosed PDFs with the FBI. *See id.* (citing 6 U.S.C. § 1503(d)(2)).

PDFs are full of 'information that identifies' a number of 'specific individuals,' it is apparent that [Subjects] did not comply with this provision of the CISA." (internal alteration omitted)); H'rg Tr. at 51:1–6 (government counsel making same point).[16] Most telling, the Subjects made clear that the 34 privileged pages at issue, though "broadly scattered," did not appear in all of the 45 PDFs, H'rg Tr. at 24:16–25:2, and thus Lawyer A could have turned over to the FBI for forensic purposes only those Disclosed PDFs without any privileged contents, but this is not what happened.[17]

Then, in an about-face from asserting they retained privilege in the Disclosed PDFs, the Subjects disavow the "authenticity" of the contents of the Disclosed PDFs, reasoning that only the holder of the privilege can waive the privilege, and because the Disclosed PDFs are primarily documents "created by Qatari-linked cyber-criminals," and "are not the [Subjects'] authentic documents," they are not really the Subjects' documents at all, so the Subjects could not have waived any privilege by providing the files to the FBI. Subjects' Mem. at 13–14.[18] The Subjects

---

[16] Even assuming the Subjects are correct that the Disclosed PDFs could not be modified in any way without sacrificing their value as evidence of the cyberattack, *see* Subjects' Reply at 7–8, 11–13, nothing in the record suggests that the Subjects contemplated the provisions of CISA when providing the Disclosed PDFs to the FBI or discussed with the FBI whether partial production of those PDFs or partial redactions of personal information or privileged information offered a way to provide solely "information . . . directly related to a cybersecurity threat." 6 U.S.C. § 1503(d)(2)(A).

[17] In any event, CISA does not require the FBI or other law enforcement agency to ignore evidence of any other crime—aside from the cyberattack—that may arise in the course of investigating a cyberattack. Indeed, other provisions of CISA suggest that criminal investigations override CISA's protections, where necessary. *See* 6 U.S.C. § 1507(n) ("Nothing in this subchapter shall be construed to prevent the disclosure of a cyber threat indicator or defensive measure shared under this subchapter in a case of criminal prosecution, when an applicable provision of Federal, State, tribal, or local law requires disclosure in such case.").

[18] Relatedly, the Subjects claim that any purported waiver by Subject 2, an attorney, cannot operate to waive [redacted] *clients'* privilege over any of the materials provided. *See* Subjects' Mem. at 17–18. This "elementary" tenet of the attorney-client privilege doctrine, *id.* at 17, is undisputed and entirely irrelevant here since the 2018 Decision's waiver ruling pertained only to emails in which (1) Subject 1, or Subject 1 and Subject 2 together, communicated with attorneys; or (2) Subject 1 and Subject 2 communicated only with one another. 2018 Decision at 18. As the holders of the attorney-client [redacted] privileges at issue, only the Subjects—and not Subject 2's clients—were covered by the waiver part of that decision. *See* Gov't's Opp'n at 8 ("The government's argument and this Court's holding regarding the waiver of privilege by [Subjects] was limited only to the privileges— attorney-client [redacted] —belonging to [Subjects]."). At the same time, any communications between or among the Subjects and/or any co-conspirators, to the extent those communications furthered the [redacted] schemes, in violation of 18 U.S.C. §§ 371, [redacted] and 22 U.S.C. §§ 611–21, for which the government had sustained

double-down on this point by contending that had contents of the Disclosed PDFs been authentic, a number of steps would have been taken to "fulfill[] basic production parameters," such as providing a unique identifier for each page. *Id.* at 14 n.10. Such steps were not taken, however, "[i]n order to preserve the integrity of the [documents] as evidence of [cyberattacks]." *Id.* "The implication is clear," according to the Subjects, Law Firm A "was willing to provide criminally-sourced, purported communications to the government, but not to produce the [Subjects'] authentic communications potentially protected by privilege." *Id.* at 15; *see also* Subjects' Reply at 1 (arguing that production of documents that "had, in turn, apparently [been] received . . . from third parties who had compiled and, in some cases, altered ostensible reproductions of the [Subjects'] stolen documents. . . . did not knowingly waive privileges that protect any of their authentic documents that might have been reflected (accurately or not) in the stolen documents"); *id.* at 4 (same).

Despite blowing much smoke about the authenticity of the Disclosed PDFs, the record, again, belies the Subjects' efforts to raise questions about the genuineness of the contents of the vast majority of those files. Even if compiled by third, unknown parties, the contents of most of those PDFs are comprised of the Subjects' stolen emails, as they themselves have attested in concurrent civil litigation claiming harm from the dissemination of their private, personal emails. *See, e.g.*, Gov't's *Ex Parte* App., Ex. 35, Subjects' Compl. ¶¶ 85, 109, 135; *id.*, Ex. 36, Subjects' FAC ¶¶ 15, 117, 119. Moreover, although Lawyer A now claims that he raised questions as to the authenticity of some of the contents of the Disclosed PDFs with the FBI throughout the

---

its *prima facie* burden in the *ex parte* application, are subject to the crime-fraud exception, which vitiates any attorney-client [redacted] privileges that may otherwise attach. *See* 2018 Decision at 24 n.2 (holding although "ample reason [exists] to believe that [Subject 2's] purported attorney-client relationships were, in fact, sham relationships set up to allow the participants to rely on the protections of the attorney-client privilege. . . . a determination that these relationships were sham relationships is not necessary in this case as the crime-fraud exception is applicable to the relevant communications").

course of his conversations with law enforcement agencies, *see* Lawyer A Decl. ¶ 32, he also affirmed to the FBI which emails were "legitimate," May 18, 2018 FBI 302, at 3. The fact that these Disclosed PDFs contained authentic personal emails is also confirmed by Lawyer B's careful redactions of potentially privileged material in a production to the OSC.[19]

In sum, the Subjects' voluntary disclosure to the FBI of the 45 PDFs containing privileged communications and information constituted an intentional waiver as to the communications contained in the Disclosed PDFs under Rule 502(a)(1). Thus, the Subjects have correctly disclaimed privilege in the Disclosed PDFs, despite citing the wrong reasons. As for the consideration, under Rule 502(a)(2), whether "the disclosed and undisclosed communications or information concern the same subject matter," the Subjects, despite their coyness in acknowledging the authenticity of the contents of the Disclosed PDFs, obviously wish to preserve privilege as to some undisclosed communications on the same subject matter as those contained in the Disclosed PDFs. The final prong of Rule 502 is addressed next.

b. The Subjects' Disclosure Does Not Operate as a Subject Matter Waiver with Respect to Undisclosed Communications Under Federal Rule of Evidence 502(a)(3)

What remains for consideration is Federal Rule of Evidence 502(a)(3), which asks whether the undisclosed and disclosed communications on the same subject matter "ought in fairness to be considered together." Reconsideration turns on this factor.

---

[19] The Subjects' effort, under the guise of a reconsideration motion, to attack the authenticity of the Disclosed PDFs may simply serve as a strategy to undermine the crime-fraud ruling. *See* Subjects' Mem. at 21 (complaining that "it is impossible to determine . . . the exact nature of the criminal or fraudulent acts alleged"). This effort is both misguided and premature, as the crime-fraud ruling was not based on the Disclosed PDFs, and, as discussed *infra* Section III.B, the Subjects have no right to delay the grand jury further by challenging the crime-fraud ruling at this procedural juncture. Moreover, parsing now which contents of the Disclosed PDFs are authentic is unnecessary, when the Subjects have muddied the issue with a veritable cacophony of arguments as to why they retain privilege in the Disclosed PDFs.

The Subjects have now shared additional factual detail concerning the disclosure of the PDFs, including that the Disclosed PDFs—created by unknown third parties and compiled from the Subjects' stolen emails (which were, in some instances, modified)—were turned over at the request of the FBI in order to relay forensic data significant to the cybersecurity investigation; and that the Subjects denied the FBI's request for access to the Subjects' email accounts and computer systems in order to preserve the confidentiality of the Subjects' communications and information. These circumstances alter the analysis as to whether undisclosed and disclosed communications ought in fairness be considered together. While the Subjects' voluntary disclosure of the Disclosed PDFs constituted a waiver as to those PDFs, this disclosure does not operate as a subject matter waiver of attorney-client privilege over the Subjects' undisclosed communications under Rule 502(a).

As recounted at length, the Subjects' actions with respect to the Disclosed PDFs' disclosure demonstrated that they did not intend to waive their privilege over undisclosed communications on the same subject matter, and this background illustrates why fairness does not require a subject matter waiver. Law Firm A advised the California USAO and FBI "on multiple occasions . . . that materials from the [Subjects] that cyberattackers had accessed and stolen were confidential and highly sensitive." Lawyer A Decl. ¶ 18. On a March 28, 2018 call, Law Firm A "expressly refused to provide access to compromised computer systems and other evidence containing internal communications. . . . explain[ing] that the content of these systems included privileged, confidential, and otherwise sensitive communication and documents." *Id.* ¶ 20. When the FBI requested that the Subjects, "through counsel at [Law Firm A], share copies of the [Disclosed PDFs]," *id.* ¶ 22, and indicated that it planned to dispatch FBI forensic investigators to copy all evidence from the Subjects' computers, Law Firm A initially reiterated

that it would not provide the content of the emails stolen in the cyberattack, *id.* ¶¶ 25–26 ("[Law Firm A] . . . ma[de] clear that any information provided would exclude any content information such as email text." (internal quotation marks and alteration omitted)). These actions demonstrate that the Subjects "did not intend to waive any privilege attaching to . . . the confidential records that were kept in the ordinary course of business." *Id.* ¶ 33.

Further, the Subjects emphasize that any actions taken with respect to the Disclosed PDFs must be viewed within the context of the ongoing criminal investigation into the cyberattack. *See* Subjects' Mem. at 18–20. Since original copies of the Disclosed PDFs may have contained forensic information vital to the cyberattack investigation, Lawyer A Decl. ¶ 23, and in light of the FBI's statement that "original evidence is best," *id.* ¶ 21, the Subjects suggest that they essentially had no way of ensuring that the FBI had the best evidence to pursue the cyberattack investigation without giving them the unaltered Disclosed PDFs. *See also id.* ¶ 29 ("The [California] USAO and FBI conveyed through their actions and statements that the only way for a criminal prosecution to occur on behalf of the [Subjects] was through the FBI's independent review of . . . PDFs containing stolen documents that were unlawfully disseminated to members of the media."). This context, the Subjects suggest, militates against a ruling that the undisclosed and disclosed communications "ought in fairness to be considered together." FED. R. EVID. 502(a)(3); *see id.* explanatory note ("[S]ubject matter waiver . . . is reserved for those unusual situations in which fairness requires a further disclosure of related, protected information, in order to prevent a selective and misleading presentation of evidence to the disadvantage of the adversary.").[20] The Court agrees.

[20] Federal Rule of Evidence 502, by its terms, only applies to attorney-client privilege but its logic, in the circumstances of this case, extends to [redacted] as well.

Although the Disclosed PDFs were voluntarily provided to the FBI and are purportedly on the same subject matter as undisclosed communications of interest to law enforcement, the circumstances regarding their disclosure weigh against finding that the disclosed and undisclosed communications "ought in fairness to be considered together." FED. R. EVID. 502(a)(3). The Subjects acceded to the FBI's request for forensic evidence in the cybersecurity investigation by providing the Disclosed PDFs, which had been passed along by media sources to the Subjects and were unredacted to preserve forensic evidence, but the Subjects denied the FBI's request for additional access to their email accounts and computer systems to protect undisclosed communications. Under these circumstances, waiver as to the Disclosed PDFs does not operate as a waiver as to undisclosed communications and information on the same subject matter.

c. The Subjects' Insinuations of Government Misconduct Are Unsupported by the Record

Only brief discussion of the Subjects' insinuations of government misconduct in connection with the Subjects' provision of the Disclosed PDFs to the FBI is warranted. In support of their claim for reconsideration and other relief, the Subjects allege that the government's conduct in this matter violated the Crime Victims' Rights Act, 18 U.S.C. § 3771(a)(8) ("CVRA"), which guarantees victims "[t]he right to be treated with fairness and with respect for the victim's dignity and privacy," and exceeded the scope of the 2018 Decision. *See* Subjects' Mem. at 23–26. Neither contention is supported by the record or is grounds for further relief.

The Subjects allege that the government violated the CVRA by using "[d]eceit and gamesmanship" to siphon information volunteered by the Subjects as victims of a cyberattack to other FBI agents who viewed the Subjects as suspects in a criminal investigation. *See id.* at 25–26. This claim ignores the timing of the events at issue: the California prosecutors and FBI

agents were unaware of any other investigation into the Subjects in early April 2018, when they requested and received the Disclosed PDFs. *See* Gov't's Opp'n at 4.[21] Although the Subjects protest that the California prosecutors and FBI agents continued to interview and work with the Subjects even after learning that they were being investigated on other grounds, *see* H'rg Tr. at 63:12–22, they also note that "consistent with our desire not to produce any privileged documents, [the FBI] got nothing more [from us] than the [Disclosed PDFs]," *id.* at 63:19–24. Moreover, the Subjects point to no provision of the CVRA, or of any other policy, that would require law enforcement to notify subjects, represented by counsel, of an ongoing grand jury investigation into their conduct simply because those same subjects have contacted law enforcement on an unrelated matter. Thus, although the Subjects fault the government for being "wholly silent" on its alleged violation of the CVRA, *see* Subjects' Reply at 10 (suggesting such silence is tantamount to a concession), they fail to acknowledge that they briefed their CVRA claims only in one footnote and two pages of their opening brief, *see* Subjects' Mem. at 6 n.5 (indicating that Subjects "reserve all rights" with respect to alleged government misconduct), *id.* at 25–26, and that their argument is based on a misperception of the government's conduct and responsibilities.

---

[21] The Subjects suggest that "[t]o the extent that the Los Angeles DOJ's and FBI's repeated requests for the [Disclosed PDFs] were motivated by other ongoing investigations rather than, as stated, to permit investigation of the Qatari attacks on the Subjects—an investigation that was inexplicably put on hold and then discontinued—the requests smack of bad faith and may implicate constitutional rights." Subjects' Mem. at 6 n.5. The government responds that "[t]he agents and prosecutors investigating the conduct that is the subject of the current grand jury investigation did not become aware of the existence of the hacking investigation until after the [Disclosed PDFs] were provided to the Los Angeles FBI Agents." Gov't's Opp'n at 4. This timing is borne out by documentation of an April 25, 2018 meeting between FBI agents concerning the Subjects' emails. *See id.*, Ex. 6, FBI Exchange of Subjects' Emails (May 4, 2018) at 3, ECF No. 26-8. This meeting took place weeks after the Subjects provided the Disclosed PDFs to the FBI. *See also* H'rg Tr. at 45:21–46:16 (government counsel explaining that the East Coast team investigating the Subjects learned of the Disclosed PDFs' disclosure to the California cyberattack team via a third-party FBI agent who was not on the case team for ether investigation). Accordingly, the Subjects' insinuations of bad faith are flatly contradicted by the record.

In one such misperception, the Subjects make much of the fact that the 2018 Decision, in its concluding paragraphs, allowed the government to confront subjects with the communications, *see* 2018 Decision at 31, but did not explicitly direct it to "take any other investigative steps needed to complete its investigation," as the government had originally sought. *See* Subjects' Reply at 14–17; 2018 Decision at 2. In particular, the Subjects apparently take umbrage that the government, in the course of investigating "layered international and domestic wire transfers of tens of millions of dollars to pay for undisclosed foreign-directed lobbying of the most powerful members of our government," Gov't's Opp'n at 1, has used the fruits of its investigation to secure a guilty plea against a defendant whose conduct contributed to the finding of the crime-fraud exception, and to file a civil forfeiture complaint related to that guilty plea, *see id.* at 7; *see also* Lawyer B. Decl., Ex. 9, Civil Action No. 18-cv-2795, Verified Compl. for Forfeiture In Rem (D.D.C. Nov. 30, 2018), at 72, ECF No. 16-1; Subjects' Mem. at 23 (complaining that the "government has referred to and relied on materials the [Subjects] contend are privileged in a recent civil forfeiture complaint"); Subjects' Reply at 14–17. Nothing about the 2018 Decision—or indeed the standard practice of federal criminal investigations—prevented the government from pursuing these steps. *See* H'rg Tr. at 54:14–17 (government counsel pointing out that 18 U.S.C. § 3322 specifically authorizes the government to use grand jury information in any civil or criminal forfeiture action). After appropriately seeking and receiving judicial guidance as to whether privileges remained intact, the government did not need to seek further judicial permission to resume its investigation, including to follow any leads from evidence uncovered upon the execution of lawfully issued search warrants or from the guilty plea of a defendant.

* * *

The 2018 Decision's waiver ruling is narrowed to find that the Subjects' provision of the Disclosed PDFs to the FBI did not amount to a subject matter waiver of the Subjects' attorney-client [redacted] privilege as to the matters discussed in the 34 pages of otherwise privileged emails contained in the Disclosed PDFs. This narrowed ruling has no effect on any communications, between or among the Subjects and/or any co-conspirators to the extent those communications furthered the [redacted] schemes, in violation of 18 U.S.C. §§ 371, [redacted] and 22 U.S.C. §§ 611–21, for which the government had sustained its *prima facie* burden in the *ex parte* application. *See* 2018 Decision at 25–27, 31.

B. The Subjects Are Not Entitled To Further Unsealing of 2018 Decision

The Subjects ask for full unsealing of the 2018 Decision, as well as the government's *ex parte* application, exhibits and any transcripts, to allow a "fair opportunity to litigate fully the issues underlying it," Subjects' Mem. at 22–23, including the basis for finding that the government made a *prima facie* showing that the crime-fraud exception vitiated the attorney-client privilege with respect to "any and all communications, past and future, made in furtherance of the crimes and schemes [violations of 18 U.S.C. §§ 371, [redacted] and 22 U.S.C. §§ 611–21]" between and among the Subjects, their co-conspirators, and "others known to be involved in the conspiracy." 2018 Decision at 27. That request is denied. Indeed, the Subjects appear to have conceded at the hearing that the better time to challenge the crime-fraud exception would be after the grand jury had "run its course." H'rg Tr. at 20:24–21:18.

The Subjects do not dispute that *ex parte*, *in camera* proceedings are a well-established process to resolve privilege disputes in time-sensitive and secretive grand jury matters. *See* Subjects' Mem. at 20–21; *United States v. Zolin*, 491 U.S. 554, 568–69 (1989); *In re Grand Jury Subpoena*, 912 F.3d 623, 632 (D.C. Cir. 2019) ("We have repeatedly approved the use of [*ex parte*] information when 'necessary to ensure the secrecy of ongoing grand jury proceedings.'"

(quoting *In re Sealed Case No. 98-3077*, 151 F.3d 1059, 1075 (D.C. Cir. 1998)). This process is designed to protect grand jury secrecy and to prevent "interruptions and delays in the grand jury process that skilled defense counsel might exploit to 'try the prosecution' even before an indictment could issue." *In re Sealed Case*, 877 F.2d at 982. Any other process would risk "saddl[ing] a grand jury with mini-trials and preliminary showings [that] would assuredly impede its investigation and frustrate the public's interest in the fair and expeditious administration of the criminal laws." *Id.* (internal quotation marks omitted) (quoting *United States v. Dionisio*, 410 U.S. 1, 17 (1973)); *see also Costello v. United States*, 350 U.S. 359, 363 (1956). The D.C. Circuit has made plain that "[w]hen a grand jury's subpoena is at stake, the standard for evaluating an exception argument must be simple enough for courts to administer swiftly and efficiently, without obstructing the grand jury's mission or squandering judicial resources." *In re Sealed Case*, 676 F.2d at 814. Moreover, in making this determination, courts "will not be able to receive a complete adversary presentation of the issues. . . . [a]ny system that requires courts to make highly refined judgments—perhaps concerning volumes of documents—will most likely collapse under its own weight." *Id.*

Notwithstanding the weight and import of this precedent, the Subjects press for an opportunity, pre-indictment, to challenge the merits of the crime-fraud exception ruling. They assert that: (1) secrecy concerns are lessened because they are already aware from their grand jury subpoenas of the substance of the grand jury investigation, *see* Subjects' Mem. at 21–22; (2) allowing the government to make a *prima facie* showing presupposes that the Subjects will eventually have a chance to rebut the showing, *id.* at 20; and (3) due process requires giving the Subjects an opportunity, pre-indictment, to "raise any factual or legal arguments or defenses" to the crime-fraud exception, *id.* at 22. None of these arguments warrants the relief sought.

First, the portions of the 2018 Decision that the Subjects seek to unseal describe a grand jury investigation that, according to the government, *see* Gov't's Opp'n at 1, is ongoing and continues to be protected by the secrecy attached to grand jury proceedings. *See McKeever v. Barr*, No. 17-5149, 2019 WL 1495027, at *2 (D.C. Cir. Apr. 5, 2019) (noting that "[t]he Supreme Court has long maintained that 'the proper functioning of our grand jury system depends upon the secrecy of grand jury proceedings.'" (quoting *Douglas Oil Co. v. Petrol Stops Nw.*, 441 U.S. 211, 218 (1979))). As the government points out, the Subjects' "claim that their receipt of a grand jury subpoena vitiates the need for grand jury secrecy. . . . is unsupported and illogical, as it would subsume the centuries' old protection of grand jury material." Gov't's Opp'n at 14. The government effectively illustrates this point with the rhetorical question of "How could a grand jury operate effectively if their mere issuance of a subpoena vitiated the veil of secrecy?" *Id.* (noting that the Subjects rely on cases which "all relate to the enforcement of grand jury subpoenas against parties . . . that were nonetheless denied access to the government's *ex parte*, *in camera* evidentiary submissions because of the need to maintain the secrecy of the grand jury proceedings"). Even if the Subjects have some notion now about the matters under investigation since they have been directed by the grand jury subpoenas to produce records related to those matters, this falls far short of demonstrating their entitlement to be privy to the full scope of those matters or the evidence collected and relayed to the Court in the *ex parte* application and exhibits, and described in the redacted portions of the 2018 Decision.

Second, the Subjects posit that since the government has had the chance to meet its *prima facie* burden that the crime-fraud exception applies, the Subjects, as privilege-holders, should now have their turn, despite the grand jury context, to intervene, obtain the underlying evidence, and litigate the vitiation of their privileges. This is simply not the governing law. *See Zolin*, 491

U.S. at 563 n.7 (noting that use of the phrase '*prima facie*' "has caused some confusion" since "the standard is used to dispel the privilege altogether *without* affording the client an opportunity to rebut the *prima facie* showing" (quoting Note, 51 Brooklyn L. Rev. 913, 918–19 (1985) (emphasis in original))). The D.C. Circuit, in *In re Sealed Case*, 676 F.2d at 814–17, for example, instructed that "[b]ecause of the need for speed and simplicity at the grand jury stage, courts should not employ a standard that requires them to hear testimony or to determine facts from conflicting evidence." *Id.* at 815 n.88. The Fourth Circuit follows a similar approach. *See, e.g.*, *In re Grand Jury Proceedings #5 Empanelled Jan. 28, 2004*, 401 F.3d 247, 251 n.2 (4th Cir. 2005) ("[W]e have explicitly held that the necessary secrecy of the grand jury process prevents the party asserting the privilege from viewing the government's *in camera* evidence."); *In re Grand Jury Proceedings, Thursday Special Grand Jury Sept. Term, 1991*, 33 F.3d 342, 351–53 (4th Cir. 1994) (rejecting, "[h]owever appealing it may sound," the argument that *in camera* submissions forming the basis of a crime-fraud ruling be released to privilege-holders who are otherwise "completely unable to answer or to refute the government's allegations" because "the government has the right to preserve the secrecy of its submission because it pertains to an on-going investigation").[22]

In urging that they be afforded the opportunity now to rebut the government's *prima facie* case, the Subjects protest that they should not be forced to wait, because "it would be ironic indeed if one who contests the lawfulness of a search and seizure were always required to acquiesce in a substantial invasion of those [privacy] interests simply to vindicate them."

---

[22] As support for their contention that they should be granted a pre-indictment opportunity to rebut the government's *prima facie* evidence, the Subjects rely on an out-of-circuit case, which expressly noted a difference in practice from that of the D.C. Circuit. *See* Subjects' Mem. at 20 (citing *Matter of Feldberg*, 862 F.2d 622, 625–26 (7th Cir. 1988) (distinguishing *In re Sealed Case*, 676 F.2d at 814–15 & n.88)). Obviously, this Court is bound by the D.C. Circuit's practice and not that of the Seventh Circuit.

Subjects' Mem. at 26 (alteration in original) (quoting *United States v. Hubbard*, 650 F.2d 293, 321 (D.C. Cir. 1980)); Subjects' Reply at 8 (same). The Subjects' reliance on *Hubbard* is misplaced, because the "substantial invasion" of privacy interests at stake in *Hubbard* was the imminent *public* release of private documents, rather than use of confidential documents in an ongoing secret grand jury investigation. In *Hubbard*, the D.C. Circuit ruled that documents introduced by defendants in a Rule 41 proceeding "for the sole purpose of demonstrating the unlawfulness [under the Fourth Amendment] of [a] search and seizure," where such documents "were not determined by the trial judge to be relevant to the crimes charged . . . were not used in the subsequent trial . . . [and] were not described or even expressly relied upon in . . . [the] decision on the suppression motion," should remain sealed. 650 F.2d at 321 (internal quotation marks omitted). The "irony inherent in the [district court's] decision to unseal [those] documents," *id.* at 322, was that individuals who wished to challenge a search and seizure as overbroad would be forced to submit documents, and have those documents potentially released to the public, in order to vindicate their right to keep such documents private. *See id.* at 321 ("[T]he act of attempting to show the excesses of the search by the extent of the documents seized . . . [will] impair the very privacy rights they seek to vindicate."). No such inherent irony exists here, as the 2018 Decision did not release the Subjects' communications to the public and they remain subject to grand jury secrecy. In the event either of the Subjects is indicted, they will have the opportunity, at a later stage of the proceedings, to attempt to vindicate any remaining privilege concerns.

Finally, in addition to arguing that the time is now ripe for the Subjects to challenge the crime-fraud exception, the Subjects contend that "[t]hey are entitled to this opportunity, as a matter of due process, particularly in the context of a crime-fraud determination of apparently

sweeping scope and breadth." Subjects' Mem. at 22. The D.C. Circuit has expressly held "without merit" the notion that Subjects have a due process entitlement to the "secret evidentiary submissions in support of the enforcement of . . . subpoenas." *In re Grand Jury Subpoena, Judith Miller*, 438 F.3d 1141, 1150 (D.C. Cir. 2006). As in *In re Grand Jury Subpoena, Judith Miller*, the Subjects here "have offered nothing to take the present grand jury investigation outside the general rule [of secrecy], let alone elevate their objections to constitutional due process status." *Id.* at 1151. The Subjects' due process argument is therefore unavailing, as "nothing in the law of the District of Columbia Circuit requires or has ever required a district court to interrupt the grand jury while a recalcitrant witness enjoys a series of mini trials over his access to materials cloaked by grand jury secrecy." *Id.*

The Subjects have failed to show that the 2018 Decision represents any deviation from the well-established process for determining whether the crime-fraud exception applies, or to offer any reason to depart from the Supreme Court and D.C. Circuit's admonitions not to "saddle a grand jury with mini-trials and preliminary showings [that] would assuredly impede its investigation and frustrate the public's interest in the fair and expeditious administration of the criminal laws." *In re Sealed Case*, 877 F.2d at 982 (quoting *Dionisio*, 410 U.S. at 17). Unsealing the crime-fraud ruling and materials now would not only jeopardize the secrecy of the ongoing grand jury investigation, but would further prolong and obstruct that time-sensitive work. "Should an indictment ultimately be returned against [Subjects], [they] may seek the exclusion of improperly obtained evidence" or pursue any credible claim of prosecutorial misconduct. *In re Sealed Case*, 877 F.2d at 982 (citing *United States v. Calandra*, 414 U.S. 338, 354 n.10 (1974)).

IV. CONCLUSION

For the foregoing reasons, the Subjects' pending motion is granted in part and denied in part. The Subjects' motion for reconsideration of the 2018 Decision's ruling that the Subjects' disclosure of the Disclosed PDFs constituted a subject matter waiver of their attorney-client [redacted] privileges as to undisclosed communications on the same subjects as in the otherwise privileged 34 pages of emails contained in the Disclosed PDFs is granted and that portion of the ruling is vacated. Likewise, the Subjects are entitled to a protective order barring the government from reviewing communications or information, other than the Disclosed PDFs, between the Subjects or between the Subjects, alone or together, with their counsel, except to the extent that such communications or information are subject to the crime-fraud exception. The Subjects' motion is otherwise denied.

The government and the Subjects are directed, within 30 days of the return of an indictment against either of the Subjects, a declination decision, or a lapse in the statute of limitations period, whichever occurs earliest, to confer and to submit a joint report advising whether any portions of either the 2018 Decision or this Memorandum Opinion may be unsealed to the public in whole or in part and, if so, proposing any redactions.

An appropriate order accompanies this Memorandum Opinion.

Date: April 18, 2019

BERYL A. HOWELL
Chief Judge

ATTACHMENT D

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THREE ACCOUNTS STORED AT PREMISES CONTROLLED BY GOOGLE, INC. FOR INVESTIGATION OF VIOLATION OF 18 U.S.C. § 1344	Misc. Action No. 18-sc-322 (BAH) Chief Judge Beryl A. Howell **FILED UNDER SEAL**

ORDER

Upon consideration of the Motion for Reconsideration Of *Ex Parte* Ruling, Unsealing and Production of Materials, Sealing, and to Quash, ECF No. 16, submitted by Elliott Broidy, individually and as a representative for Broidy Capital Management, LLC and Circinus, LLC, and [redacted], individually and on behalf of [redacted] (collectively, the "Subjects"), the memoranda and exhibits submitted in support and opposition, and the entire record herein, for the reasons stated in the accompanying Memorandum Opinion, it is hereby

ORDERED that the Subjects' motion is GRANTED IN PART and DENIED IN PART; and it is further

ORDERED that the Subjects' motion to reconsider the June 26, 2018 *ex parte* ruling ("2018 Decision") that their waiver of attorney-client and spousal privileges with respect to the communications contained in 45 PDF-formatted files that they voluntarily disclosed to the FBI in April 2018 ("Disclosed PDFs") operated as a subject matter waiver as to undisclosed privileged communications on the same subjects is GRANTED and that subject matter waiver portion of the 2018 Decision is VACATED; and it is further

ORDERED that the Subjects' motion for a protective order is GRANTED with respect to undisclosed privileged communications on the same subject matter as the Disclosed PDFs, but

only to the extent that those undisclosed privileged communications are not subject to the 2018 Decision's crime-fraud exception ruling; and it is further

ORDERED that the Subjects' motion, in all other respects, is DENIED; and it is further

ORDERED that the government and the Subjects are DIRECTED within 30 days of the return of an indictment against either of the Subjects, a declination decision, or a lapse in the statute of limitations period, whichever occurs earliest, to confer and submit a joint report advising whether any portions of either the 2018 Decision or the April 18, 2019 Memorandum Opinion accompanying this Order may be unsealed in whole or in part and, if so, proposing any redactions.

SO ORDERED.

Date: April 18, 2019

Beryl A. Howell

BERYL A. HOWELL
Chief Judge