UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	
	:	
v.	:	**Case No. 1:21-cr-719 (JEB)**
	:	
CYNTHIA BALLENGER and CHRISTOPHER PRICE,	:	
	:	
	:	
Defendants.	:	

GOVERNMENT'S OPPOSITION TO
DEFENDANTS' MOTION TO SUPPRESS FACEBOOK DATA

Defendants Cynthia Ballenger and Christopher Price move to suppress data recovered from their Facebook accounts under an authorized search warrant. ECF No. 82. The Court should deny this motion because the search warrant contained ample probable cause, the FBI complied with the requirements of the Stored Communications Act, 18 U.S.C. §§ 2701-12 and the Federal Rules of Criminal Procedure in collecting this information, and the defendants fail to state a cognizable claim under the Fourth Amendment.

FACTUAL BACKGROUND[1] AND PROCEDURAL HISTORY

On January 6, 2021, the defendants attended former President Trump's "Stop the Steal" rally, then marched to the Capitol building. After the defendants reached the Capitol grounds, made their way beyond police lines and fallen barriers, and ascended stairs to reach the Capitol building, PRICE sent a picture message to his friend with the caption, "We're just taking over the capitol." As they stood on the upper west terrace overlooking the chaos, PRICE sent a follow up text exclaiming, "Tear gas and explosions going off." After PRICE's friend instructed PRICE to

[1] These facts are derived from evidence known, collected, or obtained prior to the execution of the Facebook search warrant.

"be peaceful," PRICE responded that he looked through the window of the Capitol and someone was on the floor being administered CPR. He said it "didn't look good."

Nevertheless, the defendants decided to enter the Capitol building. They approached the Senate Wing Door, documenting their journey with photographs, and passing the utter chaos around them. The defendants entered the Capitol through a broken door at approximately 3:22 p.m. After walking through the foyer, the defendants proceeded towards the Crypt. PRICE sent more text messages to his friend stating things like, "In," "Broken glass everywhere," and "Climbing through the window." He sent a photo to the friend showing a mob of rioters filling a hallway inside the Capitol building.

After the defendants left the building, BALLENGER took to social media. She posted, for example, "We stormed the capitol" and "We totalled owed it!!" BALLENGER texted another friend bragging that her and PRICE got inside the Capitol and "Ppl are pissed!!" She too sent many photos of her and PRICE breaching the building.

On January 12, 2021, the FBI received an anonymous tip reporting that BALLENGER and PRICE were "part of the crowd that entered" the U.S. Capitol on January 6, 2021. The tip reported that BALLENGER and PRICE had posted videos taken with their cellphones on social media, but they had since removed the photos but not the comments.

In March 2021, the FBI reviewed BALLENGER's and PRICE's publicly available Facebook profiles. BALLENGER's Facebook profile confirmed that she was married to PRICE, and PRICE's Facebook profile showed a post stating that PRICE and BALLENGER had traveled from Emmitsburg, Maryland, to Union Station in Washington, DC, on January 6, 2021. A person responded to the post and asked if PRICE and BALLENGER had "[broken] any windows today?" BALLENGER replied, "mostly peaceful." Another person responded to the post and asked if Price

received "a free tour of the Capitol building today?" Ballenger responded with a thumbs up emoji, signifying a level of approval to the post.

On July 30, 2021, the defendants were charged by complaint with misdemeanor offenses. On March 8, 2022, the government filed a Superseding Information, charging the defendants with four offenses relating to their participation and involvement in the breach on the U.S. Capitol on January 6, 2021, including: entering and remaining in a restricted building or ground, in violation of 18 U.S.C. § 1752(a)(1) (Count One); disorderly and disruptive conduct in a restricted building or grounds, in violation of 18 U.S.C. § 1752(a)(2) (Count Two); disorderly conduct in a Capitol building, in violation of 40 U.S.C. § 5104(e)(2)(D) (Count Three); and parading, demonstrating, or picketing in a Capitol building, in violation of 40 U.S.C. § 5104(e)(2)(G) (Count Four). ECF No. 38.

To gather information regarding the defendants' involvement in the breach of the U.S. Capitol building, the FBI sought, and Magistrate Judge G. Michael Harvey issued, a search warrant for the defendants' Facebook accounts, on November 7, 2022. Attachment A of the Affidavit in Support of the Search Warrant specifically describes the accounts to be searched:

account number [redacted] Vanity Name "[redacted]"

account number [redacted] Vanity Name "[redacted]"

See Exh. 1. Attachment B of the Affidavit specifically lists, among the information to be seized, the contents of any available messages, other communications, photographs, videos, records, and location information associated with each account dating back to November 2020. The warrant further directed Facebook to disclose all subscriber records, login histories, identifying information, and devices associated with each account.

On December 2, 2022, the FBI received and processed the Facebook return. The government provided the processed return to the defense on January 5, 2023.

[redacted]

Thus, on February 13, 2023, the defense filed a motion for leave to file, ECF 81, a motion to suppress, ECF 81-1, a memorandum of law in support of suppression, ECF 81-2 ("Mem."), and the complete search warrant, ECF 81-3. The Court granted that motion, and deemed the motion filed. We now respond.

DISCUSSION

I. The Government Properly Sought and Obtained a Search Warrant Because the Defendants' Communications are Protected by the Stored Communications Act

A. The Stored Communications Act Encompasses the Defendants' Facebook Records

Congress enacted the Stored Communications Act, 18 U.S.C. §§ 2101-12 ("SCA"), in 1986 "to fill a gap in privacy protections for electronic stored communications, which were not protected by either existing federal statutes or the Fourth Amendment." *Republic of the Gambia v. Facebook*, 575 F. Supp. 3d 8, 14 (D.D.C. Dec. 3, 2021) (citing *Hatley v. Watts*, 917 F.3d 770, 782 (4th Cir.

2019)). With the SCA, "Congress wanted to protect electronic communications that are configured to be private, such as email and private electronic bulletin boards." *Rep. of the Gam.*, 575 F. Supp. 3d at 14 (quoting *Konop v. Hawaiian Airlines, Inc.*, 302 F.3d 868, 875 (9th Cir. 2002)). Absent the SCA, communication service providers, such as Facebook, could conceivably provide the content of messages and other forms of communications stored on their servers to the Government or other third parties without regard to the privacy of their customers. With the protections of the SCA in place, the Government in a case in federal court may only obtain such communications pursuant to a Rule 41 search warrant. 18 U.S.C. § 2703(a). Unlike the Fourth Amendment, however, the SCA does not convey suppression as a remedy. *See United States v. Gasperini*, 894 F.3d 482, 489 (2d Cir. 2018); *United States v. Carpenter*, 819 F.3d 880, 890 (6th Cir. 2016), *rev'd on other grounds*, 138 S. Ct. 2206 (2018); *United States v. Guerrero*, 768 F.3d 351, 358 (5th Cir. 2014); *United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003); *United States v. Ferguson*, 508 F. Supp. 2d 7, 10 (D.D.C. 2007). The defendants acknowledge that as well. Mem. at 21.

In their motion, the defendants argue that, although they are challenging the search warrant under the Fourth Amendment, the search warrant is deficient because it does not "follow[] the express limitations" of the SCA. Mem. at 8. For example, the defendants grapple with what constitutes backup protection under the statute. *See id.* at 9. In their view, Facebook was not storing their records "for backup protection under the [SCA]," because Facebook removed the defendants' access to their accounts sometime in August or September 2021. *Id.* at 10. This decision by Facebook, in turn, means that their records fall outside of the scope of the SCA and thus the government could not use the SCA as a basis to obtain the records. *Id.* This argument is without merit.

First, this Court has already held that records from provider-deleted accounts are protected by the SCA. In *Republic of the Gambia v. Facebook*, the African nation sought communications

contained in accounts deleted by Facebook without a warrant. 575 F. Supp. 3d at 9-10. This Court held that the SCA barred Facebook from disclosing the records because the records qualified as backups even though the company deleted the accounts. *Id.* at 12-16. This holding, the Court concluded, "comports with the SCA's legislative context" to protect electronically stored communications. *Id.* at 14. Although it is unclear if Facebook deleted the defendants' accounts in this case, rather than just restricting the defendants' access, the same logic providing a broader set of protections applies.

Second, if the defendants' argument is correct, then they would have *less* protection than otherwise available to them. As noted above, the SCA exists to create Fourth Amendment-like protections for electronic communications such as Facebook records. *Id.* Absent the SCA, the defendants' records would receive no protection from third-party intrusion and the government could obtain substantive Facebook records without a warrant. Indeed, applying the defendants' reading, "Facebook could avoid the SCA's disclosure prohibition simply by deactivating a user's account." *Id.* Applying the defendants' reading of the SCA to this case, the FBI went out of its way to obtain a search warrant that it did not need to have Facebook produce the records. Put differently, the FBI afforded the defendants with more rights than otherwise available to them. It defies logic to say that law enforcement acts unlawfully when it imparts a defendant with more rights than required by law. However, as the SCA does protect the defendants' Facebook records, the FBI required a search warrant supported with sufficient probable cause to obtain them, which the FBI did in this case.

B. The Search Warrant Thoroughly Outlined The Probable Cause To Believe The Defendants Facebook Records Contained Evidence Of A Crime

The question presented to this Court is whether the search warrant was supported by probable cause. The answer is unequivocally yes. To obtain a search warrant, a law enforcement

officer must provide a magistrate judge with an affidavit that outlines the probable cause that the location, person, or thing to be searched contains evidence of a crime. Fed. R. Crim. P. 41(d)(1). In reviewing a magistrate judge's finding of probable cause, the court must review "facts and supported opinions set out within the four corners of the affidavit." *United States v. Corleto*, 56 F.4d 169, 175 (1st Cir. 2022) (internal quotations omitted). "Probable cause requires only a probability or substantial chance of criminal activity, not an actual showing of such activity." *United States v. Valentine*, 539 F.3d 88, 93 (2d Cir. 2008). Indeed, the Supreme Court provided ample guidance of what constitutes probable cause:

> A police officer has probable cause to conduct a search when "the facts available to [him] would 'warrant a [person] of reasonable caution in the belief'" that contraband or evidence of a crime is present. *Texas v. Brown,* 460 U.S. 730, 742 (1983) (plurality opinion) (quoting *Carroll v. United States,* 267 U.S. 132, 162 (1925)); see *Safford Unified School Dist. # 1 v. Redding,* 557 U.S. 364, 370-71 (2009). The test for probable cause is not reducible to "precise definition or quantification." *Maryland v. Pringle,* 540 U.S. 366, 371 (2003). "Finely tuned standards such as proof beyond a reasonable doubt or by a preponderance of the evidence . . . have no place in the [probable-cause] decision." *Illinois v. Gates*, 462 U.S. 213, 235 (1983). All we have required is the kind of "fair probability" on which "reasonable and prudent [people,] not legal technicians, act." *Id.,* at 238, 231 (internal quotation marks omitted).

Florida v. Harris, 568 U.S. 237, 243-44 (2013). In determining whether the government has met this "practical and common-sensical" standard, the courts are to look to the totality of the circumstances. *Id.* at 244. "We have rejected rigid rules, bright-line tests, and mechanistic inquiries in favor of a more flexible, all-things-considered approach." *Id.*

To this end, the affidavit generally describes the events of January 6 to establish the shear scope of criminal conduct that occurred on that day and the bounds of the restricted area around the U.S. Capitol ahead of the special joint session of Congress. Aff. ¶¶ 6-36. The affiant explains that the FBI reviewed the defendants' publicly available Facebook pages, which contained information that the defendants may have traveled to Washington, DC and entered the U.S. Capitol

building on January 6. Aff. ¶ 38. After receiving records associated with those accounts, the FBI found information that supported the defendants' ownership of the accounts. Aff. ¶¶ 39-40. Additional investigation led the FBI to discover the defendants on surveillance footage inside the U.S. Capitol, corroborating the defendants' Facebook posts. Aff. ¶¶ 41-48. The affiant explains that the FBI made contact with an individual with personal knowledge of the defendants and that person showed the FBI various text messages further implicating the defendants with the events on January 6. Aff. ¶¶ 52-59. Lastly, the defendants themselves admitted during interviews with the FBI that they were at the U.S. Capitol on January 6. Aff. ¶¶ 60-61. In sum, the affidavit detailed specific evidence that the defendants were at the U.S. Capitol on January 6, they used their Facebook accounts to make public statements about the events of the day, and they communicated electronically through non-public means with at least one other person about January 6. Thus, the affidavit established probable cause to search the defendants' Facebook accounts – not only for copies of their statements that the government already knew existed, but also for additional unknown information as the defendants used Facebook and other media to communicate electronically about January 6. The magistrate judge agreed.

The defendants now argue that the affidavit contained insufficient probable cause to establish that they committed a crime. Mem. at 16-17. In support, defendants make various points regarding their *mens rea* on January 6, their "peaceful" conduct, and their lack of knowledge about the physical barriers surrounding the U.S. Capitol. *Id.* at 17. These arguments, however, are trial defenses and do not undermine the original finding of probable cause.

C. The Search Warrant And Its Attachments Are Sufficiently Particular And Not Overbroad

In addition to establishing probable cause that a crime occurred, a search warrant must also be particular as to what is to be searched and what evidence likely exists there. *See United States*

v. Maxwell, 920 F.2d 1028, 1031 (D.C. Cir. 1990). "As the proper scope of a warrant is confined to the breadth of the probable cause that supports it, 'the requirement of particularity is closely tied to the requirement of probable cause.'" *United States v. Smith*, 19-cr-324 (BAH), 2021 WL 2982144, at *5 (D.D.C. July 15, 2021) (quoting *United States v. Griffith*, 867 F.3d 1265, 1275 (D.C. Cir. 2017)).

Attachments ("Att.") A and B to the warrant set forth the area to be searched and the items to be seized. In Attachment A, the affiant listed two specific Facebook accounts, which the FBI became aware of during its investigation into the defendants' actions on January 6. Att. A at 1; Aff. ¶¶ 38-40. The FBI reasonably believed that these accounts would contain evidence related to January 6 because the defendants made publicly available statements about the day on those accounts. Thus, Attachment A provides particular notice as to what is actually being searched.

Attachment B, on the other hand, provides guidance as to what evidence is authorized to be seized, including categories of information permitted to be seized. First, Attachment B begins by cabining the temporal scope of the substantive materials, including comments, photographs, and videos, from November 2020 to the execution of the warrant in November 2022. Att. B at 1-4. Attachment B continues in Section II to list the items to be seized by the government. At the outset of the section, the warrant restricts the government's seizure of information to those that "constitute[] fruits, contraband, evidence, and instrumentalities of violations of [the charged offenses] as described in the affidavit . . . ." Att. B. at 5. Everything that follows is thus focused on information related to January 6. The Attachment proceeds to list a series of discrete kinds of evidence to be seized.

The defendants take ire with this list of evidentiary categories and argue that the list is overbroad and not particular. Mem. at 12-15. First, the defendants argue that information regarding their state of mind should be shielded because they have a right to talk about January 6. Mem. at

13. For this argument to be true, it would mean that all communications that all defendants have about their crimes would be unavailable to the government in the prosecution of those crimes. Insofar as the seized information shows an evolution of the defendants' views about January 6 over time, the defendants may argue at trial that the jury should not give any weight to communications made after January 6 when evaluating their state of mind. Similarly, the defendants assert that their "opinions or observations about [January 6] or their friend and acquaintance opinions are not legitimate subjects for the government monitoring." *Id.* Although this statement is generally true as it relates to speech under the First Amendment, the government may pierce this protection when it establishes probable cause that a crime was committed, and such speech constitutes evidence of the crime as it did in this case. In other words, the defendants' objections appeared tethered to proving or disproving a criminal case, rather than whether the warrant actually lacked probable cause or abided by statute or law.

The defendants next take aim with subsection (b)(ii) for not specifying the identities of unknown co-conspirators. *Id.* The affidavit outlines that people at gatherings, such as the events of January 6, use their cell phones "to communicate with other individuals about the gatherings, to coordinate with other participants at the gatherings, and to post on social media and digital forums about the gatherings." Aff. ¶ 34. The affidavit also includes numerous photographs and still frames of videos that show numerous other individuals unlawful at the U.S. Capitol on January 6. The search warrant thus appropriately sought particular evidence that could tie the defendants to other known or unknown individuals during the riot.

The defendants also believe that evidence of a conspiracy is outside the scope of the FBI's investigation into the defendants. Mem. at 14. Conspiracies by their very nature are coordinated efforts between parties to commit a principal crime. *Conspiracy*, BLACK'S LAW DICTIONARY (11th ed. 2019) ("An agreement by two or more persons to commit an unlawful act."). Any evidence

that supported the existence of a conspiracy would, by default, tend to prove the commission or attempted commission of the principal crime.

The defendants claim that Attachment B does not limit the temporal scope of the location data. *Id.* But as already noted, the warrant is directed towards evidence about January 6. By extension, this subsection targets the defendants' location on January 6 to show that they were in fact at the U.S. Capitol on that day. The specificity required for a warrant varies with the circumstances within a "practical margin of flexibility." *United States v. Shilling*, 926 F.2d 1365, 1369 (4th Cir. 1987). "Likewise, there is no flaw in the fact that the documents covered by the warrant did not have specific time periods attached." *Id.* ("The dates . . . could not have been known to the Government, and . . . documents from an earlier time may have bearing on the [] violations alleged in a later year."). Indeed, evidence predating or postdating criminal conduct may also shed light on a defendant's intent. *See, e.g.*, *United States v. Cohan*, 628 F. Supp. 2d 355, 365 (E.D.N.Y. 2009) (explaining that where a warrant lacked a date limit, prior instances of conduct predating the criminal scheme by as much as *fourteen* years would potentially be admissible) (emphasis added).

Here, the warrant particularly and specifically targeted appropriate evidence. This is completely inapposite, for example, than the case of *Maxwell*, where a one-sentence request to seize "all of which are fruits, instrumentalities, and evidence of crimes against the United States of America that is fraud by wire" was deemed overbroad. 920 F.2d at 1033. Contrary to the defendants' specious arguments, the search warrant provides ample probable cause as to the crimes committed by the defendants. The warrant also narrowly targets specific kinds of evidence that there was reason to belief would be located in the defendants' Facebook accounts.

D. The Good Faith Exception Applies

The exclusionary rule is a "judicially created remedy" that is "designed to deter police misconduct." *United States v. Leon*, 468 U.S. 897, 906, 916 (1984) (citation omitted). The Supreme Court has explained that in order to justify suppression, a case must involve police conduct that is "sufficiently deliberate that exclusion can meaningfully deter it, and sufficiently culpable that such deterrence is worth the price paid by the justice system" in suppressing evidence. *Herring v. United States*, 555 U.S. 135, 144 (2009); *see Davis v. United States*, 564 U.S. 229, 236-239 (2011).

Leon recognized a good-faith exception to the exclusionary rule in the context of search warrants: evidence should not be suppressed if officers acted in an "objectively reasonable" manner in relying on a search warrant, even if the warrant was later deemed deficient. 468 U.S. at 922. *Leon* further noted that an officer's reliance would not be objectively reasonable when a warrant was "based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable." *Id.* at 923 (citation and internal quotation marks omitted). "[T]he threshold for establishing" such a deficiency "is a high one, and it should be." *Messerschmidt v. Millender*, 565 U.S. 535, 547 (2012). "In the ordinary case, an officer cannot be expected to question the magistrate's probable-cause determination or his judgment that the form of the warrant is technically sufficient." *Leon*, 468 U.S. at 921.

The circumstances here do not remotely come close to overcoming *Leon*'s good-faith exception. As in *Messerschmidt*, it would "not have been unreasonable—based on the facts set out in [the FBI agent's] affidavit—for an officer to believe" that evidence relevant to the January 6 attack would be found on the defendants' Facebook accounts. 565 U.S. at 549. The defendant's confusing argument, once again, misses the mark, and completely avoids the application of *Leon*,

instead arguing that this Court should be solely focused on the triggering statutes permitting the warrant in the first place. *See* Mem. at 21.

II. Defendants Fail to State a Cognizable Claim Under the Fourth Amendment

In the motion, the defendants argue that the Court should suppress the Facebook return, because the Fourth Amendment to the United States Constitution prohibits against unreasonable searches, and this search constitutes an unreasonable search. The defendants argue, for example that Facebook messages are "intended for private communications," and carry with them a reasonable expectation of privacy. Mem. at 4. The defendants motion appears to conflate the reasonable expectation of privacy afforded by state actors and the Constitution and the internal workings of a private social media company.

To assert a Fourth Amendment claim, the defendant must demonstrate "a legitimate expectation of privacy in the invaded place." *Rakas v. Illinois*, 439 U.S. 128, 143 (1978). If the defendant has "no reasonable expectation of privacy" in the area searched, "no Fourth Amendment search occurred, and *ipso facto*, there was no violation of constitutional right." *Townsend v. United States*, 236 F. Supp. 3d 280, 324 (D.D.C. 2017).

On that question, the Supreme Court has held that individuals lack a reasonable expectation of privacy in business records of banks, *see Smith*, 425 U.S. at 437-43, and pen-register records of telephone companies, *see Miller*, 442 U.S. at 742-44. The Court explained that the customers in those cases "voluntarily conveyed" the information to a third-party entity "in the ordinary course of business" and, accordingly, "assumed the risk that the company would reveal [the information] to the police." *Id.* At 744 (quoting *Smith*, 425 U.S. at 442) (internal quotations omitted). That principle applies here: when the defendants created their social-media accounts on Facebook, they assumed the risk that Facebook would disclose – here pursuant to warrant – similar account-usage information. That activity reflects a "business record[]" of Facebook for which the defendants can

"assert neither ownership nor possession." *Id.* at 440; *see also United States v. Trader*, 981 F.3d 961, 968 (11th Cir. 2020) ("[E]very circuit to consider this issue decided that subscriber information disclosed during ordinary use of the internet, including internet protocol addresses and email addresses, falls within the third-party doctrine.") (collecting cases).

Moreover, that Facebook is also a social-networking platform reinforces this conclusion. Activities like the posting of content from a particular location are visible to individuals in the user's network. *See, e.g.*, Aff. ¶ 66 ("A particular user's profile page also includes a 'Wall,' which is a space where the user and his or her 'friends' can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile."). And, as disclosed in its terms of service, Facebook itself monitors those same activities. *See* FACEBOOK PRIVACY POLICY, How do we use your information?, https://www.facebook.com/privacy/policy. Given these realities, users, like the defendants, cannot assert a reasonable expectation of privacy in the account-usage information disclosed to the government. For the defendants, this information includes publicly available comments to status updates, posts on their own walls, and videos and photographs uploaded to their Facebook account.

The defendants raise a specific concern about their "private conversations and attachments [sent] through the messenger service of Facebook." Mem. at 3. This question is relatively novel in the Fourth Amendment sphere. *See, e.g.*, *United States v. Rosenow*, 50 F.4d 715, 741-44 (9th Cir. 2022) (stating that a company's own review of a defendant's private social media messages should be analyzed under the Fourth Amendment) (J. Graber dissenting). Of importance to the Fourth Amendment analysis is the fact that although the sender of the message may limit the recipient of their messages to as few as one person, Facebook still reviews the contents of the messages to conduct its business. *See* FACEBOOK PRIVACY POLICY, What information do we collect?, https://www.facebook.com/privacy/policy. When viewing Facebook's own policy and use of its

customer's private messages in conjunction with the third-party doctrine, an individual who uses Facebook, such as the defendants, "assume[] the risk that the company would reveal [the information] to the police." *Miller*, 442 U.S. at 744. This conclusion is not to say that these messages are without protection from government intrusion. *See supra* Section I. However, the conversations the defendants had through Facebook lack Fourth Amendment protection and therefore cannot seek suppression of these messages in this matter.

III. The FBI's Procedures For Reviewing Returns From A Stored Communications Act Warrant Are Sound

After obtaining an SCA warrant, unlike a warrant for a person or object, law enforcement may execute that warrant by serving it upon the target as if it were a subpoena. 18 U.S.C. § 2703(g); *see also In re Info. Associated with @gmail.com*, 2017 WL 3445634, at *21 (D.D.C. July 31, 2017). After receiving the warrant, the target provides law enforcement with a set of data, which could contain material within the scope of the warrant. The law enforcement officer must then review the data to locate "media or information consistent with the warrant." Fed. R. Crim P. 41(e)(2)(B). The purpose of this two-step procedure is not to allow the Government to obtain a general warrant. Rather, this procedure exists in acknowledgment of the extensive period of time it takes to review digital material and the inconvenience to the target of the warrant should law enforcement remain at the original location of the material. *See United States v. Ganias*, 824 F.3d 199, 230-31 (2d Cir. 2016).

Defendants argue that this structure violates the First and Fourth Amendments by allowing the Government to peer into a target's private matters. Mem. at 12, 15-16. This grave conclusion, however, fails to grapple with the inherently intrusive nature of a warrant. With a warrant, the government may enter someone's home or seize a mobile device in search of evidence of a crime. This imposition is precisely why a magistrate judge must find probable cause that the location or

object in question has or is such evidence before permitting the government to make this kind of entry into someone's life. The two-step procedure for digital material is a compromise that balances the government's interest in investigating criminal conduct with the target's privacy interests. Here, the FBI did exactly as required when it recovered the defendants' account data from Facebook and reviewed them for material listed in Attachment B.

IV. The Search Warrant Outlined The Crimes That The FBI Was Investigating

The defendants assert that the FBI lacks any authority to investigate violations of Section 1752. Mem. at 17-19. Assuming this position is correct, the defendants cite no precedent, nor is the government aware of any instances, where such an issue justifies the suppression of information seized pursuant to a warrant that is deficient in this manner. The exclusionary rule exists to punish police misconduct that violates a defendant's constitutional right. *Leon*, 468 U.S. at 916. A search warrant application coming from one federal investigative agency over another is no such violation. Further, even if this discrepancy were such a violation, the warrant still sets forth violations of 40 U.S.C. § 5104, which cures the issue.

[redacted]

[redacted]

CONCLUSION

For these reasons, the United States requests that this Court deny the defendants' motion to suppress the information seized pursuant to the Stored Communications Act warrant for their Facebook records.

Respectfully submitted,

MATTHEW M. GRAVES
UNITED STATES ATTORNEY
D.C. Bar Number 481052

/s/ Andrew Haag
ANDREW S. HAAG
Assistant United States Attorney
MA Bar No. 705425
601 D Street, N.W.
Washington, DC 20530
(202) 252-7755
Andrew.Haag@usdoj.gov

/s/ Ashley Akers
ASHLEY AKERS
Trial Attorney
MO Bar No. 69601
Detailed to the U.S. Attorney's Office
601 D Street NW
Washington, DC 20530
(202) 353-0521
Ashley.Akers@usdoj.gov

Dated February XX, 2023