UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA v. MATTHEW BLEDSOE, Defendant.	Criminal Action No. 21-204 (BAH) Chief Judge Beryl A. Howell

MEMORANDUM OPINION

On January 6, 2021, a joint session of the United States Congress convened at the United States Capitol, with then-Vice President Mike Pence presiding, to carry out the constitutional duty of certifying the vote count of the Electoral College of the 2020 Presidential Election. Every four years, since this country's first contested presidential election in 1796 and over the next 220 years, Congress's certification of the electoral college vote has marked the peaceful transition of power from one presidential administration to another, with this event respectfully observed by American citizens. Before this ritual of democracy could be completed on January 6, 2021, however, a rioting mob swarmed the Capitol grounds and breached the Capitol building, forcing Congress to halt the electoral vote count for hours. Elected representatives, congressional staff, and members of the press were then evacuated under police guard and experienced the terror of hiding from the mob. Meanwhile, many rioters celebrated this chilling historic moment by photographing and recording both themselves and others on restricted grounds surrounding and inside the Capitol Building and promptly posting their user-generated content online to various social media platforms. Given the security precautions in place daily during normal operations to prevent entry into the Capitol Building of even a single unauthorized person, this breach by hundreds of rioters on January 6, 2021, was nothing less than catastrophic.

As Americans across the country watched the events unfold at the Capitol in real-time, an investigation began to identify, arrest, and prosecute the hundreds of rioters who unlawfully entered the Capitol building and participated in the assault on the constitutional ritual of confirming the results of a presidential election. As part of that investigation, and in the context of the emergency situation at the Capitol, the Federal Bureau of Investigation ("FBI") requested from Facebook identification information for accounts using its platform to broadcast videos of this highly public event that were live-streamed or uploaded to Facebook while the account user was physically in the U.S. Capitol during the time period when the mob was storming and occupying the Capitol building. Armed with the account identifiers, in the days that followed, the FBI then sought search warrants requiring Facebook to disclose various records and content associated with the accounts that would constitute evidence of specific federal criminal law violations.

Defendant Matthew Bledsoe is the owner of one such account. He was charged and convicted by a jury, on July 21, 2022, on all five counts against him for unlawfully entering into and remaining in the U. S. Capitol and corruptly acting with the intent to obstruct, influence, and impede Congress's certification of the Electoral College vote in the 2020 election, as well as for related acts underlying his unlawful entry into and subsequent conduct within the Capitol on January 6, 2021, in violation of 18 U.S.C. §§ 1512(c)(2), 1752(a)(1), 1752(a)(2), and 40 U.S.C. §§ 5104(e)(2)(D) and 5104(e)(2)(G). *See generally* Indictment, ECF No. 23; Jury Verdict, ECF No. 219.

Before trial, defendant moved to suppress all evidence from the non-public portions of his Facebook and Instagram accounts, and any evidence and information derived from the exploitation of that evidence, obtained from the execution of a search warrant on his Facebook

and Instagram accounts ("Social Media Warrant"). Def.'s Mot. Suppress Data Recovered From Facebook and Instagram Accounts and Derivative Evid. and Info. ("Def.'s Mot.") at 1, ECF No. 182. He asserts two grounds for suppression: first, defendant argues that, under *Carpenter v. United States*, 138 S. Ct. 2206 (2018), the government's initial request to Facebook seeking identifying information of accounts broadcasting videos by persons inside the Capitol during the events of January 6 was a Fourth Amendment search and thus required a warrant, Def.'s Suppl. Mot. Suppress Data Recovered From Facebook and Instagram Accounts and Derivative Evid. and Info. ("Def.'s Suppl.") at 2–4, ECF No. 184; second, he argues that, even if obtaining the initial identifying account information from Facebook presents no Fourth Amendment violation, the Social Media Warrant lacked probable cause and the good-faith exception to the exclusionary rule does not save it, Def.'s Mot. at 2–3.

The first ground asserted by defendant raises a novel Fourth Amendment issue in this Circuit: whether an account user has a protectible Fourth Amendment interest in non-content information derived from account activity records revealing that user-generated content of a highly public event occurred at a particular location and time. During the pretrial conference, on July 15, 2022, this Court denied defendant's motion to suppress in an oral ruling, with this Memorandum Opinion to follow to explain fully why, under the unique facts and circumstances of this case, defendant has not established that he had a reasonable expectation of privacy in the non-content account information disclosed by Facebook. Min. Order (July 15, 2022). The reasoning for denial of defendant's motion to suppress is set out below.

I. BACKGROUND

The facts and procedural history below describe the information relevant to defendant's motion to suppress.

A. The January 6, 2021 Attack on the Capitol

Two months after the November 3, 2020 presidential election, on January 6, 2021, a joint session of the United States Congress convened at the Capitol to certify the vote count of the Electoral College of the 2020 Presidential Election. Gov't's Opp'n Def.'s Mot. Suppress ("Gov't's Opp'n"), Ex. A (Sealed), Aff. of FBI Special Agent Mark D. Brundage Supp. Appl. Search Warrant ("Social Media Warrant Aff.") ¶ 11, ECF No. 193-1. The joint session began at approximately 1:00 p.m., with then-Vice President Mike Pence presiding. *Id*. By 1:30 p.m., the United States House of Representatives and the United States Senate adjourned to separate chambers within the Capitol to resolve an objection raised in the joint session. *Id*. Vice President Pence continued to preside in the Senate chamber. *Id*.

As the House and Senate proceedings took place, a large crowd of protestors gathered outside the Capitol. *Id.* ¶ 12. "[T]emporary and permanent barricades were in place around the exterior of the . . . building, and [U.S. Capitol Police] were present and attempting to keep the crowd away from the Capitol building and the proceedings underway inside." *Id*. At around 1:00 p.m., the crowd "broke through the police lines, toppled the outside barricades protecting the U.S. Capitol, and pushed past . . . law enforcement officers." *Id.* ¶ 13. A group of rioters outside of the Capitol began chanting "Hang Mike Pence." *Id.* ¶ 15. The mob's violence and threats of violence then escalated.

Shortly after 2:00 p.m., multiple groups of rioters "forced entry" into the Capitol, breaking windows and assaulting members of law enforcement, and mayhem broke out inside the building. *Id.* ¶¶ 17, 19. Rioters broke windows and doors, destroyed property, stole property, and attacked federal police officers. *Id.* ¶ 19. The individuals did not come unprepared but carried weapons, including tire irons, sledgehammers, bear spray, and Tasers, and also took police equipment from overwhelmed officers, including shields and batons. *Id*.

During the ensuing chaos, law enforcement ordered then-Vice President Mike Pence, House and Senate members, and all nearby staff and reporters into the Senate and House chambers and locked down both locations. *Id.* ¶ 18. The lockdown did not deter the mob, and rioters attempted to break into the House chamber, forcing law enforcement to draw their weapons to protect the victims sheltering inside. *Id*. Subsequently, law enforcement ordered the evacuation of lawmakers from the chambers for their safety. The rioting mob persisted in seeking out and threatening members of Congress. Shortly after the evacuation, rioters broke into the office of House Speaker Nancy Pelosi. *Id.* ¶ 21. The mob also breached the Senate Chamber, and publicly available video shows an individual asking, "Where are they?" as the rioters opened the door to the Senate Chamber. *Id.* ¶ 22. In another video, a rioter can be heard asking, "Where the fuck is Nancy?" as the mob continued to scour the Senate Chamber. *Id.* ¶ 23.

Law enforcement was not able to ensure that the U.S. Capitol was cleared of the mob until 6:30 p.m. *Id.* ¶ 29. Ultimately, the mob's actions resulted in an hours-long halt to the electoral vote count while elected representatives, congressional staff, and members of the press hid in terror. The joint session, and thus the constitutional ritual of confirming the results of the 2020 Presidential Election, was "effectively suspended until shortly after 8:00 p.m." *Id.* ¶ 30.

Publicly available video footage and photographs showed that many rioters used their cell phones to record the events occurring in and around the U.S. Capitol by taking photos and videos of themselves and others, and posting them online while the attack on the Capitol Building was ongoing. In the hours and days following the riot, the identity of many rioters was unknown to law enforcement agencies, and some still remain unidentified.

B. The FBI's Emergency Disclosure Request to Facebook

To further the FBI's immediate efforts to identify those responsible for committing possible violations of federal laws within the U.S. Capitol on January 6, 2021, the FBI, observing

the open and obvious use of cell phones by many rioters to record their and others unlawful activity, sought information from Facebook, a social media platform where users can preserve and distribute photographs and videos. Specifically, on January 6, 2021, the FBI requested that Facebook identify "any users that broadcasted live videos which may have been streamed and/or uploaded to Facebook from physically within the building of the United States Capitol during the time on January 6, 2021, in which the mob had stormed and occupied the Capitol building." *Id.* ¶ 40 (footnote omitted).

In making this request to Facebook for non-content user identification information, the FBI relied on the procedures set forth in the Stored Communications Act ("SCA"), 18 U.S.C. § 2701 *et seq*. The SCA authorizes a provider of electronic communication services to disclose voluntarily records or other information related to a customer, not including the contents of any communications, "to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency." 18 U.S.C. § 2704(c)(4). According to the FBI agent who requested the information, "[b]ased on the nature of the conduct on January 6," the government held an objectively reasonable belief that "those who perpetrated the intrusion of the Capitol that day would commit other acts of violence based on apparent anger of the results of the presidential election," and thus, while at large, "posed a future danger of an emergency involving danger of death or serious physical injury." Decl. of FBI Special Agent Michael E. Hess ("Hess Decl.") ¶¶ 3, 5, ECF No. 214-1.

In response to the FBI's request, Facebook made three separate disclosures, on January 6, January 13, and January 22, 2021, voluntarily identifying Facebook and Instagram accounts that fell within the scope of the FBI's request. *Id.* ¶ 4. For each qualifying account responsible for

streaming or uploading a video to Facebook from within the U.S. Capitol building during the January 6, 2021 attack, Facebook disclosed both an Object ID, which is a unique, numeric code assigned to any video uploaded to Facebook or Instagram Live, and an associated User ID, which is a unique numeric code assigned to each Facebook or Instagram account, identifying the account that posted content indicative of being inside the U.S. Capitol building during the January 6 breach. Social Media Warrant Aff. ¶ 40 & nn.4 & 7. Subsequent searches by the FBI of the publicly available portions of Facebook and Instagram using these User IDs revealed no publicly available content associated with the accounts. *Id.* ¶¶ 43–44.

C. The Requested Warrant

Armed with the account identifiers, the FBI then sought search warrants requiring Facebook to disclose various records and information associated with the voluntarily disclosed User IDs. As relevant to this case, relying on the User IDs disclosed on January 22, 2021, the FBI requested, and on March 3, 2021, a magistrate judge approved, a warrant to search twenty-five Facebook and Instagram accounts associated with the disclosed user identifications. Gov't's Opp'n, Ex. A (Sealed), Social Media Warrant, ECF No. 193-1. The warrant specifically directed Facebook to disclose the contents of any available messages, posts, chats, or other communications, photos, videos, location history, user information, transactional records related to user account activity, and other records associated with the accounts, dating back to November 2020. *Id.* Att. B Part I at 5–9, ECF No. 193-1. The government attested that the requested records constituted evidence of violations, *inter alia*, of 18 U.S.C. §§ 1752(a)(1)–(4) (unlawful entry on restricted buildings or grounds); 1512(c)(2); (obstruction of Congress); 111 (assaulting a federal agent); 231 (civil disorders), 371 (conspiracy); 372 (conspiracy to impede/assault federal agents); 930 (possession of firearms and dangerous weapons in federal facilities); 641 (theft of government property); 1361 (destruction of government property); 2101 (interstate travel to

participate in riot); 1752(b)(1)(A) (using or carrying a weapon on restricted buildings or grounds); and 40 U.S.C. § 5104(e)(2) (violent entry, disorderly conduct, and other offenses on Capitol grounds), on January 6, 2021. *Id.* Att. B Part II at 10–11. The government explained that the requested information could be used to establish (1) the account user's identification or location, (2) the account user's state of mind "related to the criminal activity under investigation," (3) the user's breach and unlawful entry of the Capitol building, and (4) "efforts after the fact to conceal evidence of [the foregoing] offenses, or to flee prosecution for the same," among other pertinent matters. *Id*. Thus, review of such evidence would allow the FBI not only to identify perpetrators of the January 6, 2021 riot but also to establish key elements of any crimes the account users, their associates, friends, and co-conspirators committed while participating in the Capitol attack that day.

In response to the warrant, Facebook produced the requested information, and law enforcement, while reviewing the production, discovered that one of the identified Facebook accounts disclosed on January 22, 2021, was associated with defendant.

D. Relevant Procedural History

With trial in this matter initially scheduled for August 1, 2022, and a pretrial conference scheduled for July 15, 2022, the deadline for the filing of all pretrial motions was set for April 1, 2022. Scheduling Order (Feb. 2, 2022). Defendant subsequently moved to file any motions to suppress by April 29, noting that he did not believe any such motion would "require an evidentiary hearing to resolve." Def.'s Unopposed Mot. Extend Deadlines for Filing Pretrial Mots. ¶ 4, ECF No. 169; *see* Min. Order (Apr. 1, 2022) (granting the motion). On April 29, 2022, defendant filed the instant motion to suppress, as supplemented on May 1, 2022. On May 10, 2022, due to an opening in the Court's calendar, the trial was rescheduled for July 18, 2022. Min. Order (May 10, 2022). Subsequently, the government requested an extension of the

briefing schedule for the suppression motion, with such motion becoming ripe for resolution on June 3, 2022. Min. Order (May 17, 2022).

With the briefing concluded and neither party requesting an evidentiary hearing, after hearing argument on defendant's motion to suppress the Social Media Warrant at the three-hour pretrial conference on July 15, 2022, the Court issued an oral ruling denying this motion, as well as two other pretrial motions. Min. Order (July 15, 2022). Since then, both sides, with the Court's permission, have supplemented the record in support of their respective arguments in connection with the suppression motion. Gov't's Suppl. Br. Resp. Def.'s Mot. Suppress ("Gov't's Suppl."), ECF No. 211; Gov't's Notice Decl. Supp. Gov't's Opp'n Def.'s Mot. Suppress, ECF No. 214; Def.'s Unopposed Mot. Leave File Ex. Under Seal (Sealed) ("Def.'s Mot. Seal"), ECF No. 221 (filing under seal Facebook's production to the FBI in response to the Social Media Warrant ("Facebook Return")). As noted, the arguments concerning Facebook's initial voluntary disclosure to the FBI raise an issue of first impression in this Circuit, and therefore this Memorandum Opinion explains the reasons for denial of the defendant's motion to suppress the Social Media Warrant.

II. LEGAL STANDARD

The Fourth Amendment prohibits law enforcement from conducting "unreasonable searches and seizures," and provides that "no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. CONST. amend. IV. A government search found to be in violation of the Fourth Amendment's protections is generally subject to the exclusionary rule, requiring suppression of evidence obtained through unconstitutional means. *United States v. Weaver*, 808 F.3d 26, 33 (D.C. Cir. 2015) (citing *Mapp v. Ohio*, 367 U.S. 643, 655 (1961);

Weeks v. United States, 232 U.S. 383, 398 (1914)). Excluded evidence extends to both "the primary evidence obtained as a direct result of an illegal search or seizure and . . . evidence later discovered and found to be derivative of an illegality, the so-called fruit of the poisonous tree." *Utah v. Strieff*, 579 U.S. 232, 237 (2016) (cleaned up).

III. DISCUSSION

From the FBI's investigative work stemming from the January 6, 2021 riot, defendant identifies two purported Fourth Amendment violations, each of which he believes requires suppression of any evidence obtained or derived from the Facebook Return. First, defendant contends that Facebook's voluntary disclosure, pursuant to the government's emergency request, of "accounts that were being used to stream and/or upload videos by persons who may have been inside the Capitol when the events of January 6 were ongoing" violated his Fourth Amendment rights because the responsive information provided by Facebook identifying user accounts generating content "at a particular location during a specified time period" amounted to a Fourth Amendment search requiring a warrant. Def.'s Suppl. at 2–3. Second, defendant contends that the Social Media Warrant authorizing the search and seizure of data from non-public portions of his social media accounts violated the Fourth Amendment because the search of his accounts was without probable cause to believe that evidence of the alleged criminal activity would be found in his accounts. Def.'s Mot. at 4–5. Based on these arguments, defendant sought the suppression of all material from the non-public portions of his social media accounts obtained pursuant to the Social Media Warrant that the government planned to admit at trial, i.e., thirty-two exhibits sourced from the Facebook Return. Def.'s Mot. Seal at 2; *see* Gov't's Notice Exs. at 3–5, ECF No. 213 (detailing the thirty-two exhibits culled from the Facebook Return that the

government planned to admit at trial). All thirty-two exhibits were, in fact, admitted as evidence during the trial. Rough Tr. Jury Trial (July 19, 2022, Afternoon Session) at 4, 12.

Each of defendant's arguments is addressed separately below.

A. The January 22, 2021 Facebook Disclosure Was Not a Fourth Amendment Search

Defendant asserts that the government's acquisition of non-content information from Facebook, a third-party electronic communication service provider, identifying which user accounts engaged in certain activities during a specified time and at a particular location qualifies as a Fourth Amendment search. The government counters that such account-usage information implicates no protectable Fourth Amendment interest because the disclosure falls squarely within the third-party doctrine. Gov't's Opp'n at 4–6. Indeed, the Supreme Court has held repeatedly that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties," *Carpenter v. United States*, 138 S. Ct. 2206, 2216 (2018) (quoting *Smith v. Maryland*, 442 U.S. 735, 743–44 (1979)), "even if the information is revealed on the assumption that it will be used only for a limited purpose" such as "in the ordinary course of [the third-party's] business," *id.* (quoting *United States v. Miller*, 425 U.S. 435, 442–43 (1976)). Defendant seizes on the *Carpenter* decision as necessitating a finding that the third-party doctrine does not cover the acquisition of the records revealing the particular location of a user of a third-party's services during a specified time period. Def.'s Suppl. at 3. Thus, the key question presented in this case is whether, under *Carpenter*, the government's acquisition from Facebook of non-content information derived from user-generated content of a highly public event that reveals the user's location, i.e., user-generated location information ("UGLI"), was a Fourth Amendment search requiring a probable cause warrant.

After a review of the current state of the law governing the application of the Fourth Amendment to government requests for records and data that reveal location information, defendant's challenge to the data and records at issue in this case is addressed.

1. *Fourth Amendment Application to Data Revealing Location Information*

The Fourth Amendment safeguards "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. CONST. amend. IV. "Not all government actions are invasive enough to implicate the Fourth Amendment." *United States v. Warshak*, 631 F.3d 266, 284 (6th Cir. 2010). Instead, "the application of the Fourth Amendment depends on whether the person invoking its protection can claim a 'justifiable,' a 'reasonable,' or a 'legitimate expectation of privacy' that has been invaded by government action." *Smith*, 442 U.S. at 740.

To establish a legitimate expectation of privacy a defendant must demonstrate that his conduct exhibits "an actual (subjective) expectation of privacy," *id.* (quoting *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)), showing that "he seeks to preserve [something] as private," *id.* (alteration in original) (quoting *Katz*, 389 U.S. at 351), and that his subjective expectation of privacy is "one that society is prepared to recognize as 'reasonable,'" *id.* (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)). Put another way, the defendant must show that the expectation of privacy, "viewed objectively, is 'justifiable' under the circumstances." *Id.* (quoting *Katz*, 389 U.S. at 353); *see also Minnesota v. Carter*, 525 U.S. 83, 88 (1998) ("[I]n order to claim the protection of the Fourth Amendment, a defendant must demonstrate that he personally has an expectation of privacy in the place searched, and that his expectation is reasonable . . . ."). If the defendant meets that burden, then "official intrusion into that private sphere [created by a reasonable expectation of privacy] generally qualifies as a

search" under the Fourth Amendment and thus "requires a warrant supported by probable cause." *Carpenter*, 138 S. Ct. at 2213 (citing *Smith*, 442 U.S. at 740); *Brennan v. Dickson*, No. 21-1087, 2022 WL 3008030, at *7 (D.C. Cir. July 29, 2022) ("A 'search' for purposes of the Fourth Amendment occurs when government action infringes a sphere an individual seeks to preserve as private and the expectation of privacy is one society considers reasonable under the circumstances.").

To date, the Supreme Court has touched, without delving deeply into, the murky waters of navigating how the government's use of recent technological innovations should be constrained by the Fourth Amendment. In *Carpenter*, the Supreme Court took its first dive at sounding out the depths of when the government's acquisition of a specific type of digital data—personal location information maintained by a third-party—invades a person's legitimate expectation of privacy. At issue in *Carpenter* was the sufficiency, under the Fourth Amendment, of the government's use of court orders issued pursuant to the SCA, 18 U.S.C. § 2703(d), on a showing that "falls well short of the probable cause required for a warrant," *Carpenter*, 138 S. Ct. at 2221, to obtain historical cell-site location information ("CSLI") for a cell phone used by a suspect in a series of robberies, where the responsive CSLI data spanned a period of 127 days from one service provider and seven days from another provider, *id.* at 2212. The Supreme Court considered "whether the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements." *Id.* at 2211. After answering that question affirmatively, the Court further "conclude[d] that the Government must generally obtain a warrant supported by probable cause before acquiring such records." *Id.* at 2221.

These conclusions were based on the Court's finding that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI." *Id.* at 2217. Starting with the premise that "[a] person does not surrender all Fourth Amendment protection by venturing into the public sphere" but instead maintains "a reasonable expectation of privacy in the whole of their physical movements," *id.* (citing *United States v. Jones*, 565 U.S. 400, 430 (2012) (Alito, J., concurring in judgment) and *id.* at 415 (Sotomayor, J., concurring)), the Court reasoned that while society reasonably expects law enforcement to have the capability to pursue suspects "for a brief stretch," *id.*, for longer-term surveillance, "society's expectation has been that law enforcement agents and others would not . . . secretly monitor and catalogue every single movement of an individual . . . for a very long period," *id.* (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring in judgment)). The government's acquisition of CSLI in *Carpenter* violated such reasonable expectations. In total, the requested CSLI records provided "an all-encompassing record of the [cell phone] holder's whereabouts . . . , revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'" *Id.* (quoting *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring)); *see also id.* at 2218 (noting that "a cell phone . . . tracks nearly exactly the movements of its owner[,] . . . faithfully follow[ing] its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales"). In sum, the government's acquisition of the CSLI records over a lengthy period of time exposed much more than just an individual's discrete movements in the public sphere and thus presented legitimate and justifiable privacy concerns implicating Fourth Amendment protection.

Although a cell phone holder continuously reveals his location to his wireless carrier and the requested CSLI records were generated for commercial purposes, the *Carpenter* Court declined to extend the third-party doctrine to cover the cell phone location records captured through CSLI. Citing the "world of difference between the limited types of personal information" typically collected by third parties for commercial purposes "and the exhaustive chronicle of location information casually collected by wireless carriers today," *id.* at 2219, the Court examined two rationales undergirding the third-party doctrine to conclude that these considerations did not support extending the doctrine to cover the CSLI obtained on less than a probable cause showing under the circumstances. *Id.* at 2219–20; *see also id.* at 2220 ("Given the unique nature of cell phone location information, the fact that the Government obtained the information from a third party does not overcome Carpenter's claim to Fourth Amendment protection. The Government's acquisition of the cell-site records was a search within the meaning of the Fourth Amendment."). As to the first rationale, the Court explained that the holdings in *Smith* and *Miller* "did not rely solely on the act of sharing" but instead "considered the 'nature of the particular documents sought' to determine whether 'there is a legitimate "expectation of privacy" concerning their contents.'" *Id.* at 2219 (quoting *Miller*, 425 U.S. at 442); *see, e.g.*, *Miller*, 425 U.S. at 442 (holding that an individual did not have any legitimate expectation of privacy in the contents of checks given to a bank in part because "[t]he checks [were] not confidential communications but negotiable instruments to be used in commercial transactions"). In contrast to the limited amount of personal information revealed by telephone call logs, *Smith*, 442 U.S. at 742, banking transaction records, *Miller*, 425 U.S. at 442, or even location information disclosing a person's discrete journey on public thoroughfares, *United States v. Knotts*, 460 U.S. 276, 281–83 (1983), the CSLI records at issue in *Carpenter* provided

"a detailed chronicle of a person's physical presence compiled every day, every moment, over several years." *Carpenter*, 138 S. Ct. at 2220. Thus, the comprehensive and intimate nature of the CSLI records allows the government a much deeper intrusion into an individual's privacy than previous third-party doctrine cases.

As to the second rationale, the "sharing" in prior third-party cases rested on a "voluntary exposure" that the *Carpenter* Court found to be absent in the context of CSLI records. *See Knotts*, 460 U.S. at 281–82 (no reasonable expectation of privacy in public movements "voluntarily conveyed to anyone who wanted to look"); *Smith*, 442 U.S. at 744 (same for numerical information "voluntarily conveyed" to telephone companies); *Miller*, 425 U.S. at 442 (same for information "voluntarily conveyed" to banks and their employees). According to the Court, the nature of the activity generating CSLI renders its exposure *involuntary* because cell phone use is "indispensable to participation in a modern society," and cell phones generate cell-site records "without any affirmative action on the part of the user beyond powering up." *Carpenter*, 138 S. Ct. at 2220 (noting that "[v]irtually any activity on the phone generates CSLI," such that there is "no way to avoid leaving behind a trail of location data" unless an individual disconnects the phone from the network). Users cannot voluntarily assume the risk of exposure of the location information when its generation is essential, automatic, and inescapable. Thus, the *Carpenter* Court concluded that the third-party doctrine did not apply to the government's acquisition of the CSLI records at issue.

Despite limiting the long-standing third-party doctrine, the *Carpenter* Court characterized its holding as "a narrow one," *id.* at 2220, where it "decide[d] no more than the case before [it]," *id.* at 2220 n.4, further summarizing the scope of the ruling to be that "accessing seven days of CSLI constitutes a Fourth Amendment search," *id.* at 2217 n.3. The *Carpenter* Court

acknowledged that this narrow holding left open a range of questions about the application of the Fourth Amendment to CSLI, other types of data revealing location information, and "other business records that might incidentally reveal location information." *Id.* at 2220. Nevertheless, the *Carpenter* Court expressly declined to decide "whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be," *id.* at 2217 n.3, and whether individuals have a reasonable expectation of privacy in "real-time CSLI or 'tower dumps' (a download of information on all the devices that connected to a particular cell site during a particular interval)," *id.* at 2220, such that the government must seek a warrant based on probable cause before obtaining such data. *See also United States v. Green*, 981 F.3d 945, 958 (11th Cir. 2020) (noting question unresolved by Supreme Court of "whether acquiring [real-time tracking data] constitutes a search"); *United States v. Trader*, 981 F.3d 961, 968 (11th Cir. 2020) (noting Supreme Court's unresolved questions of whether "the government [can] obtain less than seven days' worth of cell-site location information without a warrant," whether "the government [can] collect cell-site location information in real time or through 'tower dumps' not focused on a single suspect" without a warrant, and whether "other [non-CSLI] business records that might incidentally reveal location information" require a warrant (cleaned up)). Following *Carpenter*, lower courts have grappled with these questions left unanswered by the Supreme Court, which has yet to take up the issue again.

Notably, in sidestepping these questions to issue a "narrow" holding, the *Carpenter* Court highlighted the context-specific nature of the Fourth Amendment's application, even in cases involving CSLI. In particular, the *Carpenter* Court took care to note that "if law enforcement is confronted with an urgent situation, such fact-specific threats will likely justify the warrantless

collection of CSLI" and emphasized that its decision "does not call into doubt warrantless access to CSLI in such circumstances." *Id.* at 2223; *see also id.* (noting that, while Carpenter's ruling requires police to "get a warrant when collecting CSLI to assist in the mine-run criminal investigation," the decision "does not limit [law enforcement's] ability to respond to an ongoing emergency"). All told, the *Carpenter* Court's limited holding embodied its caution that "no single rubric definitively resolves which expectations of privacy are entitled to protection." *Id.* at 2213–14.

2. *Defendant Lacks a Reasonable Expectation of Privacy in the UGLI Data Disclosed by Facebook*

Defendant attempts to stretch *Carpenter*'s narrow holding to cover the disclosed information at issue in this case, arguing that the government's obtainment of non-content information identifying Facebook and Instagram accounts broadcasting video content of a highly public event from a particular place and during a specified time must be considered a Fourth Amendment search under *Carpenter*'s logic. To leverage *Carpenter*'s holding to reach the non-content information at issue, defendant, not the government, must establish *Carpenter*'s applicability. *Rawlings v. Kentucky*, 448 U.S. 98, 104 (1980) ("[Defendant], of course, bears the burden of proving . . . that he had a legitimate expectation of privacy . . . ."); *United States v. Sheffield*, 832 F.3d 296, 305 (D.C. Cir. 2016) ("[D]efendants always bear the burden of establishing that the government violated a privacy interest that was protected by the Fourth Amendment."). At every turn, however, defendant fails to offer any factual support, and only sparse briefing, establishing how the requested information presents the same privacy concerns identified in *Carpenter* that rendered the third-party doctrine inapplicable to the CSLI records at issue in that case. As the burden of establishing a reasonable expectation of privacy in the social

media account records requested by the government falls on defendant, these failures are fatal to his motion.

First, defendant does not dispute, nor even address, that he voluntarily conveyed to Facebook the information contained in Facebook's disclosure to the FBI that he now seeks to suppress. Although Facebook's voluntary disclosure to the government did not provide personal location data directly to the government, the disclosed User and Object IDs were derived from location records Facebook collects from a variety of user-generated activity. Facebook's Data Policy informs users of how and when it collects information regarding account activity generated by users of its services. For example, it "collect[s] the content and other information [users] provide when [they] use [its] Services, including when [a user] sign[s] up for an account, create[s] or share[s], and message[s] or communicate[s] with others," which includes "information in or about the content [the user] provide[s], such as the location of a photo or the date a file was created." Gov't's Opp'n, Ex. B, Facebook Data Policy at 2, ECF No. 192-1. Additionally, "depending on the permissions" granted by the user, Facebook also collects "information from or about the computers, phones, or other devices where [users] install or access [its] Services," such as "device locations, including specific geographic locations, such as through GPS, Bluetooth, or WiFi signals" and "[c]onnection information such as . . . IP address[es]." *Id.*; *see also* Social Media Warrant Aff. ¶¶ 84–89 (discussing similar policies for Instagram).

Thus, unlike the CSLI data at issue in *Carpenter*, the only way that Facebook was able to determine when and where a user engaged in account activity on January 6, 2021, is by virtue of the user making an affirmative and voluntary choice to download the Facebook or Instagram application onto an electronic device, create an account on the Facebook or Instagram platform,

and, critically, take no available steps to avoid disclosing his location, before purposefully initiating the activity of live-streaming or uploading a video of a highly public event, in a manner that occurs during the normal course of using Facebook as intended. Defendant has not identified a single instance where Facebook logs information concerning his account activity of posting any photo or video content on the Facebook platform without user action.

Not only has defendant failed to show the UGLI collected by Facebook is automatic and inescapable, but he has also failed to show that Facebook usage is essential to modern life. Defendant has not attempted to place into the record any evidence establishing that Facebook "and the services [it] provide[s] are 'such a pervasive and insistent part of daily life' that [using] [its social media platform] is indispensable to participation in a modern society." *Carpenter*, 138 S. Ct. at 2220 (quoting *Riley v. California*, 573 U.S. 373, 385 (2014)).

Calling the location information embedded in and associated with, even incidentally, user-generated and posted content "UGLI data," is not just effective word play. The acronym accurately reflects the inherent and critical difference between the CSLI records in *Carpenter* and the account-usage information disclosed here: the information at issue here is affirmatively and voluntarily generated by the user, not automatically and unavoidably created simply by powering up a cell phone. The volitional aspect of the UGLI data at issue in this case "places the conduct into the heartland of the third-party doctrine recognized in *Smith* and *Miller*." Gov't's Opp'n at 8; *see United States v. Cox*, 465 F. Supp. 3d 854, 857 (N.D. Ind. 2020) ("Decisions post-*Carpenter* have noted the volitional aspect of IP address collection as a key point of distinction from CSLI."); *United States v. Kidd*, 394 F. Supp. 3d 357, 366 (S.D.N.Y. 2019) (holding that in order for a defendant to meet his burden of showing a reasonable expectation of privacy in application data linked to a defendant's cell phone, he must establish that "his cell

phone [] passively generates [the app activity records] for [the app] to collect in a way similar to CSLI"); *Sanchez v. Los Angeles Dep't of Transp.*, 39 F.4th 548, 559 (9th Cir. 2022) (distinguishing location data collected by application where the user "affirmatively chose to disclose location data" to the app provider each time he used its services, in particular because the user agreed to the app's privacy policies which expressly stated that the location data would be collected by the provider and shared with government authorities); *Trader*, 981 F.3d at 968 (noting that every circuit to consider the question pre- and post-*Carpenter* has held that subscriber information disclosed during ordinary use of the internet, including IP addresses, falls within the third-party doctrine); *id.* (collecting cases); *cf. Carpenter*, 138 S. Ct. at 2220 (noting that the voluntary-exposure rationale of the third-party doctrine did not "hold up when it comes to CSLI"). Much like the disclosure of deposit slips in *Miller*, showing that a customer utilizing the bank's services deposited money into an account at a particular bank location on a particular date, defendant, having "voluntarily conveyed" information regarding user-generated account activity, i.e., a video of a highly public event either live-streamed from or uploaded to his Facebook account during the ordinary course of using Facebook's services, cannot assert a reasonable expectation of privacy in Facebook's disclosure of that information to the government. Defendant has failed to show that Facebook's disclosure does not fall within the ambit of the third-party doctrine.

Defendant's attempt to claim a reasonable expectation of privacy in the disclosed account-usage information under the logic of *Carpenter* fails for another reason: he has not established that the disclosed information rested on "a detailed chronicl[ing] of [defendant's] physical presence compiled every day, every moment, over several years." *Palmieri v. United States*, 896 F.3d 579, 588 & n.7 (D.C. Cir. 2018) (first alteration in original) (quoting *Carpenter*,

138 S. Ct. at 2220) (noting that *Carpenter* distinguished *Smith* and *Miller* on this basis). Instead, the "nature of the particular [information] sought" by the government showcases the limited capability of the UGLI data to reveal the type of intimate personal information that the *Carpenter* Court identified as implicating serious privacy concerns. *Carpenter*, 138 S. Ct. at 2219 (quoting *Miller*, 425 U.S. at 442). The government did not ask for, nor did Facebook voluntarily disclose, the contents of any confidential messages, posts, or other communications posted by defendant. *See Miller*, 425 U.S. at 442 (noting that a defendant had a diminished expectation of privacy in records that were not confidential communications). The government also did not ask for, nor did Facebook voluntarily disclose, information that had the potential to reveal an account user's movements "beyond public thoroughfares," such as "into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Carpenter*, 138 S. Ct. at 2218.[1] Finally, the government did not ask for, nor did Facebook voluntarily disclose, a record of defendant's movements over the course of a year, a month, a week, or even a day. Instead, the requested information—user identification numbers associated with accounts that broadcasted a video of a highly public event live-streamed or uploaded while the user was in the U.S. Capitol building during a discrete time period spanning approximately 4.5 hours—was narrowly circumscribed to reveal an account user's presence in a government building (1) where ordinarily "[o]nly authorized people with appropriate identification are allowed access," Social Media Warrant Aff. ¶ 9, (2) where serious criminal conduct occurred, (3) during an unprecedented national emergency, with concomitant national security implications,

[1] Indeed, the *Carpenter* Court's reasoning evinced a heightened sensitivity for location information that "provides an intimate window into a person's life," revealing "'the privacies of life.'" *Carpenter*, 138 S. Ct. at 2217 (quoting *Riley*, 573 U.S. at 403). In contrast, the government's request and Facebook's disclosure does not carry even the smallest of risks of associating user accounts with locations or activities that expose such highly private, personal, or confidential communications, choices, or associations of the user.

(4) while the user was surrounded by a mob numbering in the hundreds (or even thousands) and was engaging in broadcasting highly public activity through a social media platform.[2] Nothing about the circumstances in which these account users found themselves even hints at an expectation of privacy in their physical location. Nor would any such expectation be one that society is prepared to accept as reasonable, especially considering the blatant criminal conduct occurring within the usually secured halls of the Capitol building during the constitutional ritual of confirming the results of a presidential election.[3] *See Brennan*, 2022 WL 3008030, at *8 ("'[R]elatively short-term monitoring of a person's movements' in public places 'accords with expectations of privacy that our society has recognized as reasonable.'" (alteration in original) (quoting *Jones*, 565 U.S. at 430 (Alito, J., concurring in judgment))); *see also Matter of Search of Info. Associated with Cellular Tel. Towers Providing Serv. to [Redacted] Stored at Premises Controlled by Verizon Wireless*, No. 21-SC-59 (BAH), 2022 WL 2922193, at *5 (D.D.C. July 25, 2022) ("[W]hether a probable cause warrant is required under the Fourth Amendment for the government to obtain 'tower dumps,' for short time periods in circumscribed locations where serious criminal conduct occurred, is murky at best, even though this investigative technique may be critical for prompt identification of a perpetrator." (citation omitted)); *United States v. Walker*, No. 2:18-CR-37-FL-1, 2020 WL 4065980, at *8 (E.D.N.C. July 20, 2020) (finding "no Fourth Amendment violation when officers obtained the orders" for CSLI, pursuant to SCA §

[2] Not only would any lawful entrants to the restricted areas of the Capitol building be required to reveal their identification to the government prior to entering, but the government continuously monitors the halls of the Capitol through CCTV cameras. *See, e.g.*, Social Media Warrant Aff. ¶ 45 (noting that U.S. Capitol CCTV footage captured an individual associated with one of the targeted Facebook accounts entering the Capitol building and walking through the crowds). Nothing is private about entry into the Capitol.

[3] In fact, in the immediate aftermath of the events of January 6, 2021, the FBI set up a "Most Wanted" webpage devoted solely to "identifying individuals who made unlawful entry into the U.S. Capitol building and committed various other alleged criminal violations," posting numerous pictures and videos of individuals on restricted grounds surrounding and inside the Capitol Building. *Most Wanted: U.S. Capitol Violence*, FED. BUREAU INVESTIGATIONS, https://www.fbi.gov/wanted/capitol-violence (last visited Aug. 21, 2022).

2703(d), for four 60- to 90-minute time periods over the course of two days, and "no basis for attaching a Fourth Amendment interest to tower dump CLSI [sic]" because such dumps only "capture CLSI [sic] for a particular *place* at a *limited time*" and therefore "the privacy concerns underpinning the court's holding in *Carpenter* do not come into play" (emphasis in original)).

Other aspects of the requested information confirm defendant's reduced expectation of privacy in the UGLI data that Facebook voluntarily disclosed to the government. Notably, Facebook's Data Policy warns users that it will "access, preserve and share information when [it] has a good faith belief it is necessary to: detect, prevent and address fraud and other illegal activity; to protect [Facebook], [the user] and others, including as part of investigations; or to prevent death or imminent bodily harm." Facebook Data Policy at 6–7. By agreeing to Facebook's Data Policy, defendant voluntarily "assumed the risk" that the company's records "would be divulged to police" should Facebook have a good faith belief that such disclosure is necessary to detect or address illegal activity. *Smith*, 442 U.S. at 745. Now finding himself in that exact situation, defendant never attempts to address the impact his voluntary agreement has on his ability to establish the serious privacy concerns raised in *Carpenter*. Moreover, defendant has not even attempted to argue or submit evidence demonstrating that Facebook's collection of UGLI for defendant's account comes to close to creating an "exhaustive chronicle of location information" that results in "near perfect surveillance" similar to the CSLI records held by wireless carriers. *Carpenter*, 138 S. Ct. at 2218–19; *see also Kidd*, 394 F. Supp. 3d at 366 (holding that a defendant must establish that a cell phone "consistently conveys granular location information" for the application to collect in order to demonstrate a reasonable expectation of privacy in UGLI data associated with a cell phone). Each of these omissions create gaping holes

in defendant's attempt to extend *Carpenter*'s coverage to the UGLI-derived account-usage information disclosed to the government in this case.

Defendant has fallen far short of demonstrating that application of the third-party doctrine to user identification information derived from UGLI data for accounts in which the users live-streamed or uploaded videos of a highly public event is inconsistent with this doctrine's underlying rationales. As the burden of establishing a reasonable expectation of privacy rests with the defendant, under the existing record, defendant has failed to establish any reasonable expectation of privacy in the disclosed account-usage records. Accordingly, defendant's failure to establish any Fourth Amendment interest in the non-content user identification information derived from UGLI data that Facebook voluntarily disclosed to the FBI means that no suppression of the contents of defendant's social media accounts is warranted on this basis.[4]

[4] Given this holding the alternative grounds proffered by the government to deny suppression of the thirty-two exhibits, Gov't's Opp'n at 9–11, 15–17, need not be addressed. Nonetheless, the government's heavy reliance on one of those alternative grounds warrants brief comment. Specifically, the government argues that, under the good-faith exception, the FBI's objectively reasonable reliance on 18 U.S.C. § 2702(c)(4)'s emergency disclosure provision renders the exclusionary rule inappropriate in this case. *Id.* at 9; *see Illinois v. Krull*, 480 U.S. 340, 349–50 (1987) (holding that the exclusionary rule should not apply to evidence "obtained by an officer acting in objectively reasonable reliance on a statute," even if the statute is later found to be unconstitutional); *Davis v. United States*, 564 U.S. 229, 241 (2011) ("[T]he harsh sanction of exclusion 'should not be applied to deter objectively reasonable law enforcement activity.'" (quoting *United States v. Leon*, 468 U.S. 897, 919 (1984))). To support this alternative ground, the government's record establishing that Facebook reasonably had a good-faith belief that an emergency existed compelling its January 22, 2021 disclosure is sparse. The FBI agent's declaration explaining the emergency circumstances prompting the initial request to Facebook contains no factual support establishing any objective reason to believe that *sixteen* days after the January 6, 2021 attack, either the FBI or Facebook reasonably believed that "law enforcement [was] confronted with an urgent situation," i.e., the need to protect congressional officers, law enforcement in the Capitol, or other individuals from threats of "imminent harm" from rioters who participated in the January 6 attack. *Carpenter*, 138 S. Ct. at 2223; *see generally* Hess Decl. Nor does the government provide any declaration from Facebook stating fact-specific reasons for why the emergency outlined in the January 6, 2021 request was considered to be ongoing through January 22, 2021. The record evidence shows that, on January 22, 2021, the FBI did not feel an urgent need to take action to identify the perpetrators of the January 6 attack based on Facebook's disclosure since the FBI waited until February 7, 2021, *sixteen* days later, to search publicly available information on the Facebook accounts associated with the disclosed User IDs and to request that Facebook preserve the contents of the identified accounts, Social Media Warrant Aff. ¶¶ 43, 47, and waited until March 3, 2021, *forty days* later, to request a warrant to search the identified accounts. These time periods raise serious questions of whether, after the dispersal of the mob that attacked the Capitol building on January 6, 2021, by the end of that day and the increased security precautions then put in place through the Inauguration, the urgent need for the information initially requested on January 6 continued until January 22, 2021, to permit the FBI's reliance on the emergency disclosure provision in § 2702(c)(4).

B. Probable Cause Supports the Social Media Warrant

Having concluded that Facebook's voluntary disclosures of *non-content* information to the FBI under the circumstances did not violate the Fourth Amendment, defendant's next Fourth Amendment challenge must be addressed. Based on his legitimate expectation of privacy in the *content* of his social media accounts that were designated "non-public" at the time of the Social Media Warrant, defendant contends that the government violated his Fourth Amendment rights by obtaining such content because the Social Media Warrant lacked probable cause. Def.'s Mot. at 4–5; *see also* Facebook Return (Sealed) at 6–11, ECF No. 223 (showing that defendant's Facebook account settings at the time of the search restricted access to his posts to himself or to Facebook Friends that he accepted). As support for this contention, defendant points to a line in the affidavit filed in support of the Social Media Warrant, stating that the FBI asked Facebook to identify "users that broadcasted live videos which *may* have been streamed and/or uploaded to Facebook from physically within the building of the United States Capitol during the time on January 6, 2021 in which the mob had stormed and occupied the Capitol building." *Id.* at 2 (emphasis in original) (quoting Social Media Warrant Aff. ¶ 40). Highlighting the use of the word "may," defendant reasons that, "at most, the Affidavit only establishes a possibility that the Facebook and Instagram accounts at issue might contain evidence of criminal activity." *Id.* at 3.

The government posits that defendant's reasonable expectation of privacy in the non-public content of his social media accounts is "open to debate," Gov't's Opp'n at 12 n.2, but, in any event, is an issue that need not be resolved because the government obtained a search warrant before accessing the contents of his social media accounts, *id*. Obtaining a warrant was a prudent approach given the weight of persuasive authority holding that non-public content held on social media accounts is protected under the Fourth Amendment. *See United States v. Westley*, No. 3:17-cr-171, 2018 WL 3448161, at *6 (D. Conn. July 17, 2018) ("Because of the

nature of a Facebook account, which allows users to post information privately, share information with select groups of 'friends,' or post information publicly, courts have held that whether the Fourth Amendment applies to a user's Facebook content 'depends, *inter alia*, on the user's privacy settings.'" (quoting *United States v. Meregildo*, 883 F. Supp. 2d 523, 525 (S.D.N.Y. 2012))); *Meregildo*, 883 F. Supp. 2d at 525 ("When a social media user disseminates his postings and information to the public, they are not protected by the Fourth Amendment. However, postings using more secure privacy settings reflect the user's intent to preserve information as private and may be constitutionally protected." (citation omitted)); *United States v. Chavez*, 423 F. Supp. 3d 194, 202–04 (W.D.N.C. 2019) (holding that a Facebook user has a reasonable expectation of privacy in content which he has intentionally excluded from public access). *But see United States v. Weber*, No. CR 21-28-M-DLC, 2022 WL 1222896, at *5 (D. Mont. Apr. 22, 2022) (holding that a defendant lacked a reasonable expectation of privacy in the content of his social media accounts because he did not introduce any evidence regarding the privacy settings for his account and the terms of service imposed by the social media platform "likely rendered any subjective expectation of privacy objectively unreasonable" as they "informed him that Instagram was monitoring his content and may provide such content to law enforcement in certain situations"). Examination of the Social Media Warrant shows that the Fourth Amendment's probable cause requirement for the searches authorized is amply satisfied.

A showing of probable cause "is not a high bar," *District of Columbia v. Wesby*, 138 S. Ct. 577, 586 (2018) (quoting *Kaley v. United States*, 571 U.S. 320, 338 (2014)), and, in the context of a search warrant, requires only a "fair probability that . . . evidence of a crime will be found in a particular place," *Illinois v. Gates*, 462 U.S. 213, 238 (1983). To evaluate whether this standard is met, courts focus on whether the warrant application provides "a 'substantial

basis' for concluding that 'a search would uncover evidence of wrongdoing'" by "demonstrat[ing] cause to believe that 'evidence is likely to be found at the place to be searched'" and that "'a nexus [exists] . . . between the item to be seized and criminal behavior.'" *United States v. Griffith*, 867 F.3d 1265, 1271 (D.C. Cir. 2017) (first alteration and omission in original) (first quoting *Gates*, 462 U.S. at 236; then quoting *Groh v. Ramirez*, 540 U.S. 551, 568 (2004); and then quoting *Warden, Md. Penitentiary v. Hayden*, 387 U.S. 294, 307 (1967)). The task of a district court reviewing a magistrate's determination that a warrant is supported by probable cause "is simply to ensure that the magistrate had a 'substantial basis for . . . conclud[ing]' that probable cause existed." *Gates*, 462 U.S. at 238–39 (alteration and omission in original) (quoting *Jones v. United States*, 362 U.S. 257, 271 (1960)).

The Social Media Warrant Affidavit provided ample reason to believe that evidence of criminal activity occurring at the U.S. Capitol on January 6, 2021 would be found in the identified social media accounts. The affidavit sets out a clear nexus between the content held in the social media accounts targeted by the search warrant and the multitude of criminal offenses committed within and around the Capitol Building. Critically, the identified social media accounts were ones found to have engaged in broadcasting video content recorded or uploaded while the user was within the Capitol Building during the time of the riot. In attacking this nexus, defendant focuses on the government's use of the word "may." This is far too thin a reed to support suppression, given the full context and the known capabilities of Facebook, including those detailed in the warrant. The affidavit provided ample grounds to believe that Facebook reliably ascertained which accounts posted content while the user was physically located in the U.S. Capitol. For example, as discussed earlier, Facebook generates IP logs for a given Facebook user, which detail "the date and time of" any account activity engaged in by a

Facebook user—like posting a video—as well as "the user ID and IP address associated with the action." Social Media Warrant Aff. ¶ 64; *see also* Facebook Data Policy at 2 (noting that Facebook collects "[c]onnection information such as . . . IP address" from "the computers, phones, or other devices where [users] install or access [its] Services"). By determining the physical location associated with the logged IP address, Facebook can easily determine the time and geographic location at which the account activity took place. Facebook also collects metadata from photos and videos uploaded by users, which "can include information . . . about the content [a user] provide[s], such as the location of a photo or the date a file was created." Facebook Data Policy at 2. These facts support the reasonable inference that Facebook has the technological capacity to confirm the particular location and time at which users upload videos. Additionally, the Social Media Warrant Affidavit described law enforcement's successful efforts to corroborate Facebook's identification of relevant accounts that posted videos from within the Capitol on January 6. Social Media Warrant Aff. ¶¶ 45–46 (noting that "[p]rior FBI investigation identified individuals associated with certain accounts sought in [the] warrant and corroborated their involvement in the offenses under investigation," including their use of Facebook to post photos and videos while unlawfully remaining in the Capitol).

Based on Facebook's identifications, law enforcement had a solid basis and good reason to believe that the identified social media accounts would contain incriminating information relevant to the crimes committed during the attack on the Capitol on January 6, especially as news footage of the attack showed rioters taking photos and videos of themselves and others breaking into the Capitol, damaging and stealing property from within the building, and attacking law enforcement as the mob impeded the certification of the Electoral College vote. *Id.* ¶¶ 34–39. In sum, the issuing judge had a reasonable basis to conclude that evidence of

criminal activity occurring during January 6, 2021, would be found in the social media accounts identified by Facebook.[5]

IV. CONCLUSION

For the reasons stated above, as supplemented by the Court's oral ruling on July 15, 2022, the defendant's Motion to Suppress Data Recovered from Facebook and Instagram Accounts and Derivative Evidence and Information, ECF No. 182, is **DENIED**.

SO ORDERED.

Date: August 22, 2022

BERYL A. HOWELL
Chief Judge

[5] In the alternative, even if the Social Media Warrant lacked probable cause, under the good-faith exception, exclusion of the seized evidence from non-public portions of defendant's social media accounts is not warranted. Under the logic of the good-faith exception, "'evidence seized in reasonable, good-faith reliance on a search warrant' need not be excluded, even if the warrant turns out to have been unsupported by probable cause," *Griffith*, 867 F.3d at 1278 (quoting *Leon*, 468 U.S. at 905), so long as the warrant is not "based on an affidavit so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable," *Leon*, 468 U.S. at 923 (cleaned up). Here, the Social Media Warrant Affidavit is not so lacking in indicia of probable cause as to warrant suppression. As detailed in the text, this affidavit articulated specific facts detailing the nature of criminal activity and describing the connection between the identified accounts and the unlawful conduct occurring on January 6, thereby providing a reasonable basis for believing that the social media accounts would hold evidence of the criminal activity under investigation. Social Media Warrant Aff. at 7–15. Additionally, the affidavit provided factual support for the government's reasonable reliance on Facebook accurately identifying accounts that broadcasted content from within the Capitol during the January 6 attack, including additional corroborating evidence not provided by Facebook. *Id.* ¶¶ 45–46, 54, 64–65, 72. Probable cause does not require knowledge to a near-certainty, and here the government provided more than sufficient support to believe that Facebook, the owner of the social media platforms which hosted the content at issue, was capable of determining the time and location account activity took place on its site.