**UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF COLUMBIA**

| | | |
|---|---|---|
| **UNITED STATES OF AMERICA** | : | |
| | : | |
| **v.** | : | **Case No. 21-CR-204 (BAH)** |
| | : | |
| **MATTHEW BLEDSOE,** | : | |
| | : | |
| **Defendant.** | : | |

**GOVERNMENT'S OPPOSITION TO DEFENDANT BLEDSOE'S MOTION TO SUPPRESS FACEBOOK AND INSTAGRAM DATA**

The United States respectfully opposes defendant Matthew Bledsoe's motion to suppress data recovered from his Facebook and Instagram accounts. ECF 182 & 184. Bledsoe has failed to show that the government violated the Fourth Amendment in collecting this information.

**BACKGROUND**

The grand jury charged Bledsoe with crimes related to his participation in the events of January 6, 2021, at the U.S. Capitol. Bledsoe and a mass of other individuals congregated outside the Capitol building as a Joint Session of Congress convened inside. ECF 179 at 2 (Gov't Opp. to Mot. to Dismiss). At the Capitol's exterior door, Bledsoe appeared on video stating: "In the Capitol! This is our house! We pay for this shit! Where's those pieces of shit at?" *Id.* Bledsoe then entered the Crypt and, as various individuals attacked a line of officers, he recorded the crowd chanting, "Stop the steal! Stop the steal!" *Id.* Bledsoe then went to the Rotunda and took a selfie-style video saying, "Free Alex Jones! Look at our House! This motherfucker is nice! Holy shit! Our House!" *Id.* He also climbed the statue of Gerald Ford and walked through the Capitol building with other rioters. *Id.*

That same day, Bledsoe posted a compilation of videos at various locations around the U.S. Capitol: walking to the rally and stating "[w]e're coming" and "[j]ust the beginning," posing with

other rioters on the street (captioned "We're not gonna take it"), and displaying people as they climbed the wall at the Capitol (captioned "Nothing can stop whats [sic] coming"). *Id.* at 2-3.

The grand jury charged Bledsoe with one count each of obstructing an official proceeding and aiding and abetting the same (18 U.S.C. § 1512(c)(2)); entering and remaining in a restricting building or grounds (18 U.S.C. § 1752(a)(1)); engaging in disorderly conduct in a restricted building or ground (18 U.S.C. § 1752(a)(2)); engaging in disorderly conduct in a U.S. Capitol building (40 U.S.C. § 5104(e)(2)(D)); and parading, demonstrating, or picketing in a U.S. Capitol building (40 U.S.C. § 5104(e)(2)(G)). ECF 23.

As part of its effort to identify individuals who breached the U.S. Capitol building on January 6, the government requested and obtained from Facebook information about account users who uploaded video content from inside the U.S. Capitol building. The search warrant affidavit, *In re Information Associated with 25 Accounts Stored at Facebook*, 1:21-sc-686 (Mar. 3, 2021) (filed under seal as Ex. A) ("Aff."), summarizes the government's investigatory steps leading to Bledsoe's identification.

News footage and other public media outlets captured many individuals using cell phones to photograph or record themselves and others breaking into the U.S. Capitol on January 6. Aff. ¶¶ 36-37. Law enforcement believed that these individuals might have used social-media platforms to preserve and distribute their photographs and videos. Aff. ¶ 39.

The FBI requested that Facebook identify any users who broadcasted live videos which may have been streamed or uploaded to Facebook while the user was physically located within the U.S. Capitol building on January 6, 2021 during the time in which the mob had stormed and occupied it. Aff. ¶ 40. Starting on January 6, Facebook voluntarily identified accounts on its platforms (Facebook and Instagram) that fell within the scope of the FBI's request. Aff. ¶ 40 &

nn.5-6. At the time, published Facebook policy advised users that the company collected the content that each user "create[d] or share[d]" on his or her account, including "information in or about the content …, such as the location of a photo" and "[d]evice locations." Facebook Data Policy p.2 (Sept. 29, 2016) (attached as Ex. B). Facebook further advised users that the company "may … access, preserve and share information when [it] ha[d] a good faith belief it [was] necessary to detect, prevent and address fraud or other illegal activity; to protect [Facebook], [the user] and others, including as part of investigations; or to prevent death or imminent bodily harm." *Id.* pp.6-7; *see generally* 18 U.S.C. § 2702(c)(4) (providing that a telecommunications provider may disclose subscriber information "to a government entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires such disclosure without delay").

As relevant here, on January 22, 2021, Facebook disclosed to the government a list of 25 user identifications—consisting of a unique numeric code—that appeared to have posted such videos on their accounts. Aff. ¶¶ 40, 48. Law enforcement subsequently searched the Facebook and Instagram websites but located no publicly available content associated with those user identifications. Aff. ¶¶ ¶ 43-44.

On March 3, 2021, a magistrate judge approved a warrant to search the Facebook and Instagram accounts associated with these 25 user identifications. The warrant specifically directed Facebook to disclose the contents of any available messages, other communications, photos, 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.

In response to the warrant, Facebook disclosed information pertaining to Facebook and Instagram accounts associated with Bledsoe. Bledsoe now moves to suppress this evidence and any information derived from it.

## ARGUMENT

The Court should deny Bledsoe's motion to suppress. Because Facebook's initial voluntary disclosure of account-usage information did not constitute a government search, it did not implicate the Fourth Amendment. And law enforcement's subsequent search of Bledsoe's Facebook and Instagram accounts was supported by probable cause and authorized by warrant.

### A. Facebook's voluntary disclosure of account-usage information did not implicate the Fourth Amendment.

The Supreme Court "has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Smith v. Maryland*, 442 U.S. 735, 744 (1979) (quoting *United States v. Miller*, 425 U.S. 435, 443 (1976)). That principle forecloses Bledsoe's objection (ECF 184) to Facebook's voluntary disclosure to the government.

#### 1. Bledsoe lacked a reasonable expectation of privacy in the fact that his social-medial accounts were used from inside the U.S. Capitol on January 6.

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 742-744, and pen-register records

of telephone companies, *see Miller*, 442 U.S. at 437-443. 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." *Smith*, 425 U.S. at 744 (quoting *Miller*, 425 U.S. at 442). That principle applies here: when Bledsoe created his social-media accounts on Facebook and Instagram, he assumed the risk that Facebook would disclose similar account-usage information. That activity reflects a "business record[]" of Facebook for which Bledsoe can "assert neither ownership nor possession." *Miller*, 425 U.S. 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).

In this case, Facebook's disclosure informed the government that Bledsoe's accounts had hosted live videos that had been streamed or uploaded from the Capitol building on January 6, 2021.[1] This disclosure is the modern-day equivalent of the deposit slip in *Miller* showing that a customer deposited money into an account at a particular bank on a particular date, or the pen register in *Smith* showing that a person dialed a particular number on a particular date from the customer's home-telephone line. *See Heeger v. Facebook, Inc.*, 509 F. Supp. 3d 1182, 1190 (N.D. Cal. 2020) ("[T]he allegation that Facebook collected 'IP addresses showing locations where plaintiff Heeger accessed his Facebook account' describes a practice akin to a pen register recording the outgoing phone numbers dialed on a landline telephone.") (brackets and citation

[1] Facebook did not disclose the videos or other content at this juncture. As Bledsoe concedes, the disclosed information showed only that the "Facebook and Instagram accounts were being used by persons at a particular location." ECF 184 at 2.

omitted). Consistent with *Miller* and *Smith*, Bledsoe cannot assert a reasonable expectation of privacy in such account-usage information.

That Facebook and Instagram are social-networking platforms reinforces this conclusion. Activities like the posting of content from a particular location are visible to individuals in the user's network. *See* Aff. ¶ 53 ("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."); *id.* ¶ 81 ("Instagram allow users to post and share various types of user content, including photos, videos, captions, comments, and other materials."). And, as Facebook's terms of service disclose to users, the company itself monitors those same activities. *See* Facebook Data Policy pp. 1-2. Given this circumstance, a user like Bledsoe cannot assert a reasonable expectation of privacy in the account-usage information disclosed to the government here: the fact that a video was streamed or uploaded to his Facebook or Instagram page from a particular location.

**2. *Carpenter* is inapplicable.**

Bledsoe contends that Facebook's voluntary disclosure of this information constitutes a search under the Supreme Court's decision in *Carpenter v. United States*, 138 S. Ct. 2206 (2018). That contention lacks merit.

*Carpenter* held that the government's actions in accessing seven days of cell-site location information data constituted a Fourth Amendment search. 138 S. Ct. at 2217 & n.3. Although cell-site records are created and maintained by third-party wireless carriers, *see id.* at 2219, the Court "decline[d] to extend *Smith* and *Miller* to cover the[] novel circumstances" at issue in *Carpenter*, *id.* at 2217. The Court emphasized "the unique nature of cell phone location records," which provide "a detailed and comprehensive record of the person's [physical] movements"

resulting in "near perfect surveillance, as if [the government] had attached an ankle monitor to the phone's user." *Id.* at 2217-2218; *see id.* at 2220 (describing information in *Carpenter* as "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years").

*Carpenter* emphasized, however, that the decision was "a narrow one" and did not "disturb the application of *Smith* and *Miller*" to other types of information. 138 S. Ct. at 2220. And here, "the nature of the particular [information] sought" from Facebook, *id.* at 2219 (citation omitted)—a user identification number associated with an account that hosted a live U.S. Capitol video—is far more similar to the business records at issue in *Miller* and *Smith* than to the "detailed and comprehensive record of the person's movements" at issue in *Carpenter*, *id.* at 2217, because the information did "not capture the whole of Bledsoe's physical movements." *United States v. Soybel*, 13 F.4th 584, 592 (7th Cir. 2021). Indeed, the information here is *less private* than the personal banking records in *Miller* or the home-phone dialing information in *Smith* because the user shared the video with others on his Facebook and Instagram pages. The government's actions in requesting account-usage records from Facebook accordingly did not constitute a Fourth Amendment search under *Carpenter*.

In response, Bledsoe observes (ECF 184 at 3) that the government obtained "the location of the person who was using a Facebook account and an Instagram account … at the time the events of January 6 were ongoing." But mere disclosure of location data in a discrete hours-long period does not implicate *Carpenter*'s holding. *See United States v. Adkinson*, 916 F.3d 605, 611 (7th Cir. 2019) (*Carpenter* inapplicable to identification of cell phones "near one location … at one time") (emphasis omitted). A bank record, for instance, may show that a customer withdrew money from a particular branch or ATM on a particular date and time. But, under *Smith*, the customer lacks a reasonable expectation of privacy in that record. To constitute a Fourth

Amendment search under *Carpenter*, the disclosure must provide the government with "a detailed and comprehensive record of the person's movements." 138 S. Ct. at 2217. Facebook's disclosures here plainly did not.

Bledsoe further analogizes (ECF 184 at 3) Facebook's disclosures to a "tower dump," where a telecommunications company identifies all devices that connected to a particular cell site during a particular interval. This analogy is flawed because, unlike a tower dump, a posted Facebook video requires "an[] affirmative act on the part of the user" to connect with the platform and upload content. *Carpenter*, 138 S. Ct. at 2220; *see also United States v. Gratkowski*, 964 F.3d 307, 312 (5th Cir. 2020) (distinguishing *Carpenter* because "transferring and receiving Bitcoin requires an 'affirmative act' by the Bitcoin address holder"); *United States v. Hood*, 920 F.3d 87, 92 (1st Cir. 2019) (same for IP information because "an internet user generates the IP address data … only by making the affirmative decision to access a website or application"). In addition, unlike a tower dump, the user anticipates that content posted to his Facebook account will be "'shared' as one normally understands the term." *Carpenter*, 138 S. Ct. at 2220. This "voluntary exposure" places the conduct into the heartland of the third-party doctrine recognized in *Smith* and *Miller*. *Id.*

But even accepting Bledsoe's analogy on its face, *Carpenter* made clear that its holding did not cover "tower dumps," 138 S. Ct. at 2220—as every lower court to review the decision has recognized. *See*, *e.g.*, *Trader*, 981 F.3d at 968; *Adkinson*, 916 F.3d at 611; *In re Use of a Cell-Site Simulator*, 531 F. Supp. 3d 1, 6 n.5 (D.D.C. 2021); *United States v. Walker*, 2020 WL 4065980, at *7 (W.D.N.C. Jul. 20, 2020); *United State v. Rhodes*, 2021 WL 1541050, at *2 (N.D. Ga. Apr. 20, 2021); *see also Soybel*, 13 F.4th at 593-594 (distinguishing *Carpenter* and holding that warrantless acquisition of user's IP address remains permissible under third-party doctrine); *Hood*, 920 F.3d

at 92 (same); *United States v. Contreras*, 905 F.3d 853, 857 (5th Cir. 2018) (same). In short, *Carpenter* lends no support to Bledsoe's assertion of a privacy interest in Facebook's voluntary disclosures in this case.

**3. The good-faith exception independently forecloses relief.**

Even assuming the government's acquisition of the 25 user identifications qualifies as an impermissible warrantless search under *Carpenter*, the resulting evidence was admissible pursuant to the good-faith exception.

As the Supreme Court has explained, the exclusionary rule is a "'judicially created remedy'" "designed to deter police misconduct rather than to punish the errors of judges and magistrates." *United States v. Leon*, 468 U.S. 897, 906, 916 (1984) (citation omitted); *see Davis v. United States*, 564 U.S. 229, 236-237 (2011). It permits "the harsh sanction of exclusion only when [police practices] are deliberate enough to yield 'meaningful' deterrence, and culpable enough to be 'worth the price paid by the justice system.'" *Davis*, 564 U.S. at 240 (brackets and citation omitted). Accordingly, in *Illinois v. Krull*, 480 U.S. 340 (1987), the Supreme Court held that the good-faith exception to suppression applies when "officers act[ed] in objectively reasonable reliance upon a *statute* authorizing warrantless administrative searches," even though that statute was later found to violate the Fourth Amendment. *Id.* at 342; *see id.* at 349.

The good-faith exception likewise applies in Bledsoe's case because the FBI acted in objectively reasonable reliance on 18 U.S.C. § 2702(c)(4) when requesting a list of Facebook user identifications for accounts that had hosted live videos of the January 6 attack.

Providers must generally keep communications confidential unless a court order, warrant, or subpoena is produced. But Section 2702(c)(4) authorizes providers to disclose customer records to a governmental entity without a warrant "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."

Such is the case here. The facts underlying the U.S. Capitol attack on January 6 "would lead a reasonable, experienced officer[] to believe that there was an urgent need to take action" and immediately identify those involved. *United States v. Gilliam*, 842 F.3d 801, 804 (2d Cir. 2016) (alteration omitted). As documented in the warrant affidavit, a violent mob broke through police barriers and breached the U.S. Capitol building as a joint session of Congress convened to certify the results of the 2020 Presidential Election. Members of the mob carried weapons (such as tire irons, sledgehammers, bear spray, and Tasers), wore tactical vests, and carried flex cuffs. Aff. ¶¶ 19, 25. They threatened to harm Vice President Pence and Speaker Pelosi, *see* Aff. ¶ 15 ("Hang Mike Pence."), ¶ 23 ("Where the f*** is Nancy?"), and brutally assaulted law-enforcement officers assigned to protect the complex, Aff. ¶ 19. This attack required the evacuation of members of Congress, prompted the issuance of a city-wide curfew, and delayed formal certification of the election. Aff. ¶¶ 20, 26, 31, 32. "Lives were lost; blood was shed; portions of the Capitol building were badly damaged; and the lives of members of the House and Senate, as well as aides, staffers, and others who were working in the building, were endangered." *Trump v. Thompson*, 20 F.4th 10, 35-36 (D.C. Cir. 2021). Simply put, "[t]he peaceful transfer of power—one of [this country's] most important and sacred democratic processes—came under a full-fledged assault." *United States v. Little*, No. 1:21-cr-315, 2022 WL 768685, at *1 (D.D.C. Mar. 14, 2022).

These facts support the objectively reasonable belief that individuals who breached the U.S. Capitol on January 6 presented a realistic threat to this country's elected leaders and congressional staff—particularly because many of them were scheduled to convene at the same location for the Presidential Inauguration two weeks later. *See, e.g.*, *United States v. Pezzola*, 531

F. Supp. 3d 139, 143 (D.D.C. 2021) (noting that the Proud Boys national chairman "posted a photograph of [the defendant] and other Proud Boys to his social-media account, with the caption 'Lords of War,' and the hashtags '#J6' and '#J20'"—a likely reference to "'the dates of Congressional certification of the Electoral College vote and the Presidential Inauguration'"); *United States v. Chansley*, 525 F. Supp. 3d 151, 156 (D.D.C. 2021) (noting that the defendant informed the FBI that "Vice President Pence is a child-trafficking traitor" and "expressed his interest in returning to Washington, D.C. for the 46th Presidential Inauguration"). The FBI accordingly had a good-faith basis to request, and Facebook had a good-faith basis to disclose, user identifications associated with accounts that had hosted live videos inside the U.S. Capitol. Such information would help identify the individuals who witnessed or participated in the attack. In this instance, where a federal statute authorized the warrantless disclosure of the information in response to an emergency, application of the exclusionary rule would be inappropriate under *Krull*.

**B. Probable cause supported the warrant-authorized search of Bledsoe's social-media accounts.**

After receiving the user identification numbers from Facebook, the government sought, and the magistrate judge issued, a search warrant for the associated Facebook and Instagram accounts—including two accounts registered to Bledsoe. Bledsoe alleges (ECF 182 at 3-5) that the warrant affidavit failed to articulate probable cause and, accordingly, moves to suppress all evidence recovered from the search of his accounts. The Court should deny this claim as well.

**1. The warrant affidavit supplied ample cause to believe that the search would uncover evidence of crimes at the U.S. Capitol on January 6.**

Bledsoe challenges probable cause on one ground. In his view, the warrant affidavit established only a speculative "possib[ility] that [his Facebook and Instagram] accounts were used

to stream and/or upload videos … by someone who may have been inside the [U.S. Capitol] building" on January 6. ECF 182, at 4-5 (emphasis omitted).[2] This contention lacks merit.

The probable-cause standard "is not a high bar," *District of Columbia v. Wesby*, 138 S. Ct. 577, 586 (2018) (citation omitted), and "is less than a preponderance of the evidence," *United States v. Burnett*, 827 F.3d 1108, 1114 (D.C. Cir. 2016). In the context of a search warrant, a magistrate need only determine whether "reasonable inferences" from the evidence described in the warrant application establish a "fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238, 240 (1983). Because the probable-cause standard deals not "with hard certainties, but with probabilities," *id.* at 231 (citation omitted), the facts presented to the magistrate need only "'warrant a person of reasonable caution in the belief' that contraband or evidence of a crime is present," *Florida v. Harris*, 568 U.S. 237, 243 (2013) (brackets and citation omitted).

The warrant affidavit in this case easily passes muster. It articulated ample facts showing a fair probability that Bledsoe's social-media accounts had hosted videos streamed or uploaded from the U.S. Capitol during the January 6 attack.

First, the affidavit stated that Facebook itself had identified 25 accounts that had posted video content indicating that it had been filmed inside the U.S. Capitol, Aff ¶ 40, at a time when the Capitol was closed to the public and entry was restricted due to the ongoing certification proceedings, Aff. ¶¶ 10, 16. The magistrate judge could fairly infer that Facebook—as owner of

---

[2] Bledsoe asserts that individuals have an expectation of privacy in the contents of their social-media posts. *See* ECF 182 at 4 (citing *United States v. Chavez*, 423 F. Supp. 3d 194, 203-05 (W.D.N.C.)). That contention is open to debate. *See United States v. Palmieri*, 72 F. Supp. 3d 191, 210 (D.D.C. 2014) ("Because Palmieri had no reasonable expectation of privacy in the information he made available to 'friends' on his Facebook page, he cannot claim a Fourth Amendment violation."). But this question is not presented here because the government obtained a search warrant *before* accessing the contents of Bledsoe's accounts.

the social-media platforms—had the capacity to monitor user-posted videos and review their content.

Second, the affidavit identified various methods by which Facebook could identify a user's location. It explained that Facebook stores user-generated content (like photos and videos) on its servers indefinitely. Aff. ¶ 56. Those "photos and videos … may include any metadata such as location that the user transmitted when s/he uploaded the photo or video." Aff. ¶ 54. The affidavit further explained that Facebook logs the user's IP address and, depending on account privacy settings, the physical location of the user's device based on GPS coordinates as the user interacts with Facebook's platform. Aff. ¶¶ 64-65; *see also id.* ¶¶ 84-89 (discussing Instagram accounts). These facts corroborate the inference that Facebook had the technological capacity to confirm the particular location from where the user uploaded the video.

Third, the affidavit documented law enforcement's effort to substantiate Facebook's information. *See Gates*, 462 U.S. at 241 (observing that the Supreme Court's probable-cause decisions "have consistently recognized the value of corroboration of details of an informant's tip by independent police work"). Of the 25 user identifications disclosed by Facebook, the FBI collected evidence linking five users to the January 6 attack. Aff. ¶¶ 45-46. This corroboration further bolsters the magistrate judge's probable-cause finding.

In response, Bledsoe characterizes (ECF 182 at 5) the affidavit as "merely establish[ing] a possibility that th[e] Facebook and Instagram accounts might contain evidence of criminal activity." That is plainly incorrect. As the preceding discussion shows, the affidavit documented a fair probability that Bledsoe's social-media accounts would contain video evidence of the January 6 attack at the U.S. Capitol building. That record, combined with the "great deference"

afforded to the issuing magistrate's determination, *Gates*, 462 U.S. at 236 (citation omitted), leads to only one conclusion: probable cause supported the warrant.

**2. The good-faith exception independently forecloses relief.**

Even assuming that probable cause was lacking, the good-faith exception forecloses application of the exclusionary rule in this case.

The exclusionary rule is a "'judicially created remedy"' that is "designed to deter police misconduct." *Leon*, 468 U.S. at 906, 916 (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*, 564 U.S. at 236-239.

*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 squarely invite *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 Bledsoe's social-media accounts. 565 U.S. at 549. The affidavit clearly articulated a fair probability—based on Facebook's voluntary representations, the technological capacities of its platforms, and the government's corroboration efforts—that a video filmed from inside the U.S. Capitol had been posted to Bledsoe's accounts.

The officers who executed this warrant thus reasonably relied on the magistrate-approved warrant. Bledsoe's cursory statements to the contrary (ECF 182 at 6) fail to show otherwise.

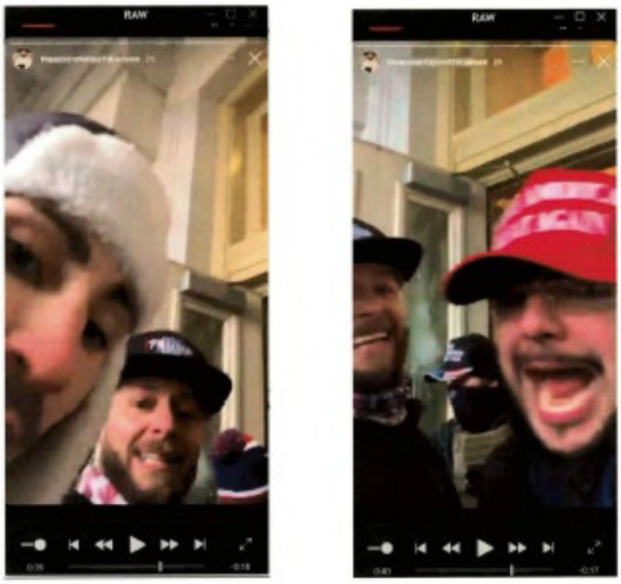
**C. The independent-source and inevitable-discovery doctrines separately establish the admissibility of the evidence collected from Bledsoe's social-medial accounts.**

Two additional doctrines counsel against suppression of the evidence collected from Bledsoe's social-medial accounts.

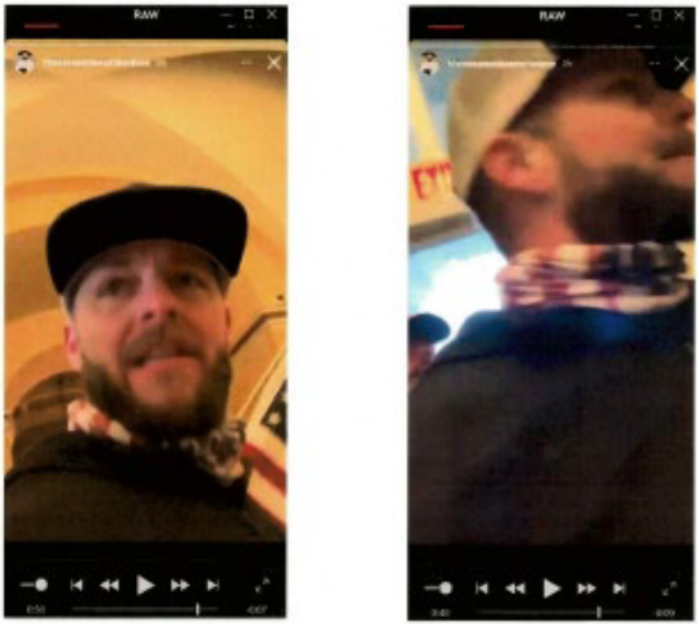
1. Under the independent-source doctrine, evidence seized pursuant to a search warrant may be admissible even when that evidence was previously discovered during an illegal search. *Murray v. United States*, 487 U.S. 533, 536-541 (1988). The rationale: when law enforcement officers have an independent source for challenged evidence, they should be placed in no worse a position than if the unlawful conduct had not occurred. *Id.* at 537; *see also Utah v. Strieff*, 136 S. Ct. 2056, 2061 (2016) ("[T]he independent source doctrine allows trial courts to admit evidence obtained in an unlawful search if officers independently acquired it from a separate, independent source."). In applying the independent-source doctrine, "[t]he ultimate question … is whether the search pursuant to warrant was in fact a genuinely independent source of the information and tangible evidence at issue here." *Murray*, 487 U.S. at 542.

As the warrant affidavit supporting the separate search of Bledsoe's residence detailed, a tipster provided the government with a copy of the compilation video that had been posted to Bledsoe's Instagram account. *See In re Search of Residence in Cordova, Tennessee*, 21-sw-19

(Jan. 14, 2021) (attached as Ex. C), ¶ 12. The video depicts Bledsoe entering the U.S. Capitol on January 6, 2021:



*Id.* ¶ 14. And the video then shows Bledsoe inside the U.S. Capitol building.



*Id.* ¶ 15. Because the government obtained this Instagram video from a source unconnected to the Facebook disclosures and search disputed in Bledsoe's motion, it is admissible at trial under the

independent-source doctrine. *See Palmieri v. United States*, 896 F.3d 579, 588 (D.C. Cir. 2018) ("Obtaining from [a third] person information [the defendant] knowingly and voluntarily shared with his Facebook friends is not a search.").

2. "[T]he inevitable discovery doctrine allows for the admission of evidence that would have been discovered even without the unconstitutional source." *Strieff*, 136 S. Ct. at 2061 (2016). The government bears the burden to show by a preponderance of the evidence that the evidence sought to be suppressed would have been discovered by lawful means. *Nix v. Williams*, 467 U.S. 431, 444 (1984). The government can easily meet that burden here. As explained above, a tipster provided the government with an Instagram video compilation showing that Bledsoe entered the U.S. Capitol building on January 6 alongside other members of the mob. The government would have sought, and a magistrate judge would have approved, a warrant to search Bledsoe's social-media accounts based on that video. It establishes probable cause to believe that Bledsoe participated in the January 6 attack and that evidence of his criminal activity (and that of those around him) would be found on his social-media accounts.

## CONCLUSION

The motion to suppress should be denied.

Respectfully submitted,

MATTHEW M. GRAVES
United States Attorney
DC Bar No. 481052

By: /s/ Melanie L. Alsworth
Melanie L. Alsworth
Trial Attorney, Detailee
Ark. Bar No. 2002095
601 D Street, NW
Washington, DC 20530
(202) 598-2285
Melanie.Alsworth2@usdoj.gov

Jamie Carter
Assistant United States Attorney
D.C. Bar No. 1027970
601 D Street, N.W.
Washington, DC 20530
(202) 252-6741
Jamie.Carter@usdoj.gov