UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA v. ASHRAF AL SAFOO, a/k/a Abu Al'-Abbas Al-Iraqi, a/k/a Abu Shanab, a/k/a Abbusi	No. 18 CR 696 Hon. John Robert Blakey

GOVERNMENT'S RESPONSE TO DEFENDANT'S PRETRIAL MOTIONS

The United States of America, by and through its attorney, MORRIS PASQUAL, Acting United States Attorney for the Northern District of Illinois, hereby respectfully submits this response in opposition to defendant's Consolidated Pretrial Motions. R. 372.

On April 24, 2014, less than a month before trial, the defendant filed a 72-page brief containing motions to dismiss each count of the indictment, a motion to quash a search warrant and a motion to suppress evidence. The motions were filed late, without good cause and without permission of the Court. In addition, the motions misstate the facts and the applicable law. For these reasons, the motions should be denied.

I. DEFENDANT'S MOTIONS ARE UNTIMELY

A. Procedural History

On November 15, 2018, the defendant was charged by indictment with multiple offenses pertaining to the provision of material support to ISIS, a designated Foreign Terrorist Organization ("FTO). R. 25. Defendant was appointed counsel from the Federal Defenders Office. Shortly after, attorneys Thomas Durkin and Joshua Herman filed notices of appearances (R. 29 and R. 30) and the defendant's initially appointed attorneys withdrew their representation.

The indictment was superseded twice (R. 132 and R. 161) and the trial date of October 5, 2020, was reset to April 12, 2021. R. 191. The Court ordered pretrial motions to be filed by November 30, 2020. R. 191. The filing deadline was extended to December 11, 2020. R. 212. On or about December 14, 2020, the defendant filed multiple pretrials motions. R. 216 – 223. On January 28, 2021, after striking the trial date due to COVID, the Court gave the defendant until March 19, 2021, to file any additional substantive pretrial motions. R. 235. No additional motions were filed.

After multiple trial dates set and continued, on February 18, 2022, at the request of the defendant, Messers. Durkin and Herman withdrew as counsel. R. 317. On April 6, 2022, Patrick Boyle was appointed to represent the defendant. R. 320. On July 13, 2022, the Court gave new counsel until September 2, 2022, to file any pretrial motions. R. 325. The filing date was extended multiple times with a final date of January 3, 2023. R. 336. At that time, trial was scheduled for February 5, 2024. R. 336.

On January 3, 2023, the defendant filed multiple pretrial motions including a Motion for Bill of Particulars and two Motions to Dismiss. R. 339 through R. 441. On May 11, 2023, attorney James Vanzant was appointed as co-counsel. R. 356.

The February 5, 2024, trial date was moved up to December 4, 2023, then back to November 11, 2024. Due to a subsequent opening in the Court's schedule, and at the request of the parties, the trial was moved forward to May 20, 2024.

At an April 24, 2024, status conference, the defendant stated that he intended to file a pretrial motion to related to the whether Twitter's servers were "protected computers" under 18 U.S.C. § 1030. The defendant had not provided the government with any prior notice of his intention to file any additional pretrial motion. The Court directed the defendant to file the motion by April 29, 2024. R. 370.

On April 30, 2024, the defendant filed a 72-page document. R. 372. The filing contained within it four Motions to Dismiss the counts in the indictment (motions that were not duplicative of the previously filed Motions to Dismiss), a Motion to Quash the Search Warrant, and a Motion to Suppress Evidence.

B. The Motions Are Untimely

The defendant's April 30 filing is untimely and was filed without a showing of good cause or leave of the Court. Pursuant to Fed. R. Crim. Pr. 12(c), it is procedurally defective.

The motion was filed almost 16 months after the Court imposed a filing deadline of January 3, 2023. In addition, the timing of the filing violated the Court's standing order which directs that, if there are no filing dates scheduled by the Court (which there were), substantive motions, to included motions to dismiss, suppress or

quash, must be filed no later than 45 days prior to the pre-trial conference. The final pre-trial conference was scheduled for May 13, 2024. 45 days prior would have been March 30, 2024. The motions were filed 30 days later.

Additionally, the motions were filed without leave of the Court. The defendant represented, during the April 24, 2024, status conference, that it would be filing a motion to suppress pertaining to Twitter. The Court allowed the filing of that motion but the defendant never sought leave to file, three weeks prior to trial, four motions to dismiss, which contain wide-ranging arguments related to the constitutionality of the statutes charged, a motion to quash and a motion to suppress.

The defendant has not presented any good cause for the late filings. The motions are not based on new information or evidence that was not already in the possession of the defendant prior to the January 3, 2023, filing deadline, nor are they based on the appointment of new counsel. Although Mr. Van Zant was appointed five months after the January 3, 2023 filing deadline, he was appointed almost one year prior to May 2024 trial date. Counsel could have sought, but never did, leave from the Court to file motions months ago, in plenty of time for the government to respond and the Court to rule prior to the May 20 trial date.

There is no good cause for the defendant to have waited 16 months past the filing deadline to file the motions. Moreover, there is no good cause why the defendant could not have filed leave with the Court to file the motions prior to the April 24, 2024, status conference. Had the government been aware of the nature and volume of the motions, it would have objected to the request to file multiple substantive

motions – based information that had been in the defendant's possession for years – a mere three weeks prior to trial.

C. Federal Rule of Criminal Procedure, Rule 12(c)

Fed. R. Crim. Pr. 12(b)(3)(B) requires a defendant to file motions to suppress and motions for failure to state an offense, prior to trial. The Court may set a deadline to file motions and the Court may extend the deadline as it sees fit. Fed. R. Crim. Pr. 12(c)(1) and (2). If a defendant does not file motion to suppress or a motion to dismiss based on a failure to state an offense by the filing deadline set by the Court, the motion is untimely, unless the defendant shows good cause for the late filing. Fed. R. Crim. Pr. 12(a)(3)(B) and 12(c)(3).

Here, the defendant filed a motion to suppress, a motion to quash the search warrant (effectively a motion to suppress), and multiple motions to dismiss based on various grounds, including constitutional challenges and failure to state and offense. The motions were filed after the Court's deadline and the defendant has failed to establish good cause for the late filing of any of the motions.

A late filed motion may be denied if no good cause for the late filing is shown. *United States v. Suggs*, 703 Fed. Appx. 425, 428 (7th Cir. 2017); *United States v. Adame,* 827 F.3d 637, 647 (7th Cir. 2016) ("If a defendant fails to file a pretrial motion to suppress, then he or she must file a motion for relief in the district court showing 'good cause' for why the district court should excuse the timeliness issue."); *United States v. McMillan*, 786 F.3d 630, 636 (7th Cir. 2015)("Federal Rule of Criminal Procedure 12(c)(3) imposes an antecedent good-cause requirement when a defendant fails to file a timely motion to suppress. Before a court may consider an untimely

motion to suppress, 'a defendant must first establish good cause for the absence of a pretrial motion.'")(cleaned up); *United States v. Glover*, No. 18 CR 643, 2019 WL 3287843, at *1 (N.D. Ill. July 22, 2019) "The defendant must establish good cause before a court may consider an untimely motion to suppress."); *United States v. Johnson*, No. 17 CR 603, 2019 WL 1331827 at *1 (N.D. Ill. March 25, 2019) (Regarding post-suppression hearing filings, Judge Kendall held that "Post-hearing position papers were due on February 18, 2019 and any responses were due by February 25, 2019. Johnson' counsel filed his position paper on March 12, 2019 and filed an affidavit in support three days later, without seeking an extension of time or otherwise acknowledging that his filings were nearly a month late. Though the Court would be within its discretion to refuse to accept Johnson's untimely submission, it will consider the filings in this instance."); *United States v. Hill*, No. 22-2400, 2023 WL 2810289, at *1 (7th Cir. Apr. 6, 2023) (The defendant file a motion to dismiss ten months after the filing deadline. "The court denied Hill's motion as untimely, without good cause for the delay, and meritless."

In *United States v. Adkinson*, 916 F.3d 605, 609 (7th Cir. 2019), the defendant file a motion for change of venue on the morning of trial. The district court denied the motion as being untimely and 30 days overdue. "Adkinson's motion came too late because Adkinson did not abide by the court's schedule and offered no reason for his tardiness or failure to comply with the district court's pretrial scheduling order." *Id.*

The government acknowledges that the trial date continuance has partially mitigated the prejudice caused by the late filings. However, the defendant's filing is

sufficiently late that the statute of limitations for certain counts in the operative indictment has lapsed. Counts Two and Three charge conspiracy, in violation of Title 18, United States Code, Section 371. Both counts charge conduct that ended in October 2018. Counts Four, Six, Eight and Ten charge unauthorized access of a protected computer, in violation of Title 18, United States Code, Section 1030. Each of these counts charge conduct that ended in September 2018. All six counts have five-year statute of limitations. The limitations period for these counts expired in September and October 2023. If the Court were to grant the motions to dismiss any of these charges, the government is unable to return to the grand jury. The defendant has had all discovery related to the filed motions for many years. Had he filed these motions by January 3, 2023 as ordered by the court, there would have been sufficient time for the court to rule on the motions and, if needed, for the government to return to the grand jury before the expiration of the limitations period.

The defendant has failed to state a good cause (or any cause) for his late motions. "The pretrial motions requirement embodied in Rule 12 serves 'an important social policy and not a narrow, finicky procedural requirement." *Salahuddin*, 509 F.3d 858 at 862. Without good cause, pursuant to Fed. R. Crim. Pr. 12(c)(3), the Court has the authority and discretion to deny the motions. However, the defendant's motions fail for the additional substantive reasons described below, which provide additional bases for denial of the motions.

II. INDICTMENT PLEADING REQUIREMENTS

An indictment satisfies constitutional requirements, including for vagueness, and the requirements of Rule 7(c) of the Federal Rules of Criminal Procedure, if it:

"(1) states the elements of the offense charged; (2) fairly informs the defendant of the nature of the charge so that he may prepare a defense; and (3) enables him to plead an acquittal or conviction as a bar against future prosecutions for the same offense." *United States v. McLeczynsky*, 296 F.3d 634, 636 (7th Cir. 2002) (*citing Hamling v. United States*, 418 U.S. 87, 117, 94 S.Ct. 2887, 41 L.Ed.2d 590 (1974). "It is generally sufficient that an indictment set forth the offense in the words of the statute itself, as long as 'those words themselves fully, directly, and expressly, without any uncertainty or ambiguity, set forth all of the elements necessary to constitute the offense intended to be punished.'" *Id*. (citations omitted). "The indictment should be read in its entirety, construed according to common sense, and interpreted to include facts which are necessarily implied." *United States v. Givens*, 767 F.2d 574, 584 (9th Cir. 1985), cert denied, 474 U.S. 953 (1985) (citation omitted); *see also United States v. Smith,* 230 F.3d 300, at 305 (7th Cir. 2000) ("Indictments are reviewed on a practical basis and in their entirety, rather than "in a hypertechnical manner.") (citation omitted). "The sufficiency of the indictment is not a question of whether it could have been more definite or certain." *United States v. Debrow*, 346 U.S. 374, 378 (1953).

III. DEFENDANT'S MOTION TO DISMISS COUNTS ONE, FIVE, SEVEN, NINE AND ELEVEN

The Supreme Court has upheld the constitutionality of Title 18, United States Code, Section 2339B (Section 2339B). *Holder v Humanitarian Law Project,* 561 U.S. 1 (2010) ("*HLP*"). The Court specifically held that the prohibition on providing material support, including services, to designated FTOs, was not impermissibly

vague, and that though the First Amendment protected "independent advocacy," it did not protect conduct, or speech, done at the direction of, or in coordination with FTOs. The defendant's arguments to the contrary lack merit. *See* Br. at 8. In summary, the defendant argues that (1) the material support statute is unconstitutionally vague, (2) defendant's actions were protected expression under the First Amendment, and (3) the allegations do not establish that defendant's actions were done "in coordination with or at the direction of" a foreign terrorist organization. The defendant's constitutional challenges are foreclosed by *HLP*, and his remaining arguments are factual issues to be resolved at trial. The motion to dismiss should be denied.

A. Factual Background

Count One charges the defendant with conspiracy to provide material support to ISIS. As alleged, the defendant conspired with other members of Khattab Media Foundation to provide material support to ISIS by taking direction from ISIS in creating and disseminating pro-ISIS information including edited video content and infographics created with video and photo editing and other similar software. R. 161 ¶ 6. Khattab posted its materials across various social media platforms. *Id.* ¶ 8.

At trial, the government expects the evidence will show that ISIS had an official media office, that ISIS prioritized media to support ISIS's goals, and that the media office explicitly targeted supporters, like defendant, who could provide additional resources to further ISIS's cause. Testimony and evidence will show that Khattab's work was in concert with this strategy and that the organization acted at the direction and control, or in coordination with, ISIS.

In addition, Counts Five, Seven, Nine and Eleven allege that the defendant provided and attempted to provide material support to ISIS through his use of Twitter Accounts A, B, C, and D. At trial the government's evidence will show that Twitter and other social media companies routinely removed posts containing terrorist or violent extremist content and suspended the related accounts. To circumvent these restrictions and maximize the reach of their posts, the defendant and other ISIS supporters shared techniques for gaining unauthorized access to Twitter by recreating defunct email accounts and using those accounts to reset the passwords to associated Twitter accounts. As alleged, the defendant used this technique to gain unauthorized access to Twitter accounts and used that access to post pro-ISIS information.

B. Argument

HLP and its progeny have uniformly found that Section 2339B is neither unconstitutionally vague nor overbroad. The defendant cites no authority to the contrary. In *HLP,* plaintiffs who wished to facilitate the lawful, nonviolent purposes of designated FTOs brought a pre-enforcement challenge to § 2339B. They sought to engage in "political advocacy" on behalf of FTOs and argued that § 2339B's prohibition on providing material support to such organizations was unconstitutional on two grounds: (1) the statute violated their freedom of speech and freedom of association under the First Amendment, and (2) the statute's prohibitions on providing "training," "expert advice or assistance," "service," and "personnel" was "impermissibly vague." *Id.* at 10-11.

The Supreme Court rejected these claims. *HLP* held that § 2339B was constitutional, even as applied to the "lawful, nonviolent" support plaintiffs wished to provide. *Id.* at 7. The Court noted that to violate the material support statute, "a person must have knowledge that the organization is a designated terrorist organization . . . , that the organization has engaged or engages in terrorist activity . . . , or that the organization has engaged or engages in terrorism." *Id.* at 16 (citing § 2339B). This prohibition, *HLP* explained, is "on its face, a preventive measure—it criminalizes not terrorist attacks themselves, but aid that makes the attacks more likely to occur." *Id.* at 35.

Regarding plaintiffs' claim that § 2339B was impermissibly vague, *HLP* held that the prohibition on providing services to an FTO was not impermissibly vague. *Id.* at 20-21. *HLP* explained that "[o]nly if the statute fails to provide a person of ordinary intelligence fair notice of what is prohibited or is so standardless that it authorizes or encourages seriously discriminatory enforcement" would a vagueness finding be appropriate. *Id.* at 18. "Services," *HLP* continued, refer to "concerted activity, not independent advocacy," and Section 2339B's requirement that the "service" be rendered "to" an FTO "indicates a connection between the service and the foreign group." *Id.* at 24. Further noting that services are defined as "performance of work commanded or paid for by another: a servant's duty: attendance on a superior" or "an act done for the benefit or at the command of another," *HLP* held that "context confirms that ordinary meaning here." *Id.* at 23–24.

Accordingly, *HLP* concluded that "a person of ordinary intelligence" "would understand the term 'service' to cover advocacy performed in coordination with, or at the direction of, a foreign terrorist organization." *Id.* at 24. At the same time, *HLP* recognized that the statutory prohibition on providing material support in the form of services did not extend to advocacy undertaken "*entirely* independently of the foreign terrorist organization" (emphasis added). *Id.* at 23; *see also id.* at 31 ("Independent advocacy that might be viewed as promoting the group's legitimacy is not covered.").

HLP further upheld the constitutionality of § 2339B on First Amendment grounds, holding that Congress had not sought to suppress ideas or opinions in the form of "pure political speech." *Id.* at 26. Rather, Congress had carefully drawn § 2339B to cover "only a narrow category of speech to, under the direction of, or in coordination with foreign groups that the speaker knows to be terrorist organizations." *Id.* at 26. Thus, *HLP* held that plaintiffs' desire to "provide support for the humanitarian and political activities of [FTOs] in the form of monetary contributions, other tangible aid, legal training, and political advocacy" was within Congress's power to prohibit. *Id.* at 10; 33-34.

HLP also noted that § 2339B did not criminalize "mere membership" in an FTO but instead prohibited providing "material support" to that group. *Id.* at 18. And it clarified that material support could include any manner of support, even forms of support that might otherwise be permissible under the law, because designated FTOs "'are so tainted by their criminal conduct that *any contribution to such an*

organization facilitates that conduct'" (quoting the Antiterrorism and Effective Death Penalty Act § 301(a)(7), 110 Stat. at 1247) (emphasis in original)); *see also United States v. Farhane*, 634 F.3d 127, 140-141 (2d Cir. 2011) (defendant's "offer to serve as an on-call doctor for [al Qaeda], standing ready to treat wounded mujahideen in Saudi Arabia, falls squarely within the core of" conduct prohibited by Section 2339B).

HLP further observed that "[p]roviding foreign terrorist groups with material support *in any form* also furthers terrorism by straining the United States' relationships with its allies and undermining cooperative efforts between nations to prevent terrorist attacks." *Id.* at 32 (emphasis added). Indeed, in considering the terrorist activities of the FTOs at issue in *HLP*, the Supreme Court found that the "taint of such violent activities is so great that working in coordination with or at the command of the [FTOs] serves to legitimize and further their terrorist means." *Id.* at 30 (cleaned up).

Despite this precedent, the defendant argues that the statute is void on its face and overbroad. Br. at 8-11. In *United States v. Farhane*, the Second Circuit rejected an argument that Section 2339B was facially vague and overbroad. 634 F.3d 127, 137 (2d Cir. 2011). Consistent with *HLP*, *Farhane* held that "the statute leaves persons free to 'say anything they wish on any topic,' including terrorism," *Id*. Because the statute does not punish "mere membership in or association with terrorist organizations," it does not "suppress … 'pure political speech". *Id*. Thus, the court found that Section 2339B was neither "facially vague in violation of due process [nor]

overbroad in violation of the First Amendment." *Id.* at 138. This case requires no different conclusion.

The defendant also argues that the statute is unconstitutionally vague as applied to him. Other courts have rejected nearly identical challenges. For example, in *United States v. Osadzinski*, defendant was charged with creating, using, sharing and teaching a computer program to save and organize ISIS materials. The defendant moved to dismiss the indictment, arguing that the conduct was protected under the First Amendment and that § 2339B was unconstitutionally vague as applied to him because a reasonable person would not know that the charged conduct was covered by Section 2339B. The district court denied the motion. *United States v. Osadzinski*, 2021 WL 3209671, at *3 (N.D. Ill. July 29, 2021), aff'd, 97 F.4th 484 (7th Cir. 2024). Citing *HLP*, the district court noted the difference between independent advocacy (protected speech) and "advocacy performed in coordination with, or at the direction of, a foreign terrorist organization" (unprotected speech). *Id.* at 3. The court noted that *HLP* clarified that when material support takes the form of speech, § 2339B "is carefully drawn to cover only a narrow category of speech, to, under the direction of, or in coordination with foreign groups that the speaker knows to be a terrorist organization." *Id.* The district court also cited *Boim v. Quranic Literacy Institute and Holy Land Foundation for Relief and Development*, 291 F.3d 1000, 1026 (7th Cir. 2002), where this Court held that "[u]nder Section 2339B . . . [defendants] may, with impunity, become members of [an FTO], praise [an FTO] for its use of terrorism, and

vigorously advocate the goals and philosophies of [an FTO]" but that § 2339B prohibits "the provision of material support . . . to a terrorist organization." App. 5-6.

In light of this precedent, the district court concluded that the "creati[on of] a computer script" that assisted ISIS's media goals was within the scope of § 2339B. *Osadzinski*, 2021 WL 3209671, at *3. The allegations here are similar. The defendant and his coconspirators were members and leaders of an organization that created and disseminated a variety of pro-ISIS materials, used social media to expand the reach of those materials, and did so at ISIS's direction. That the alleged conduct could constitute protected speech in the abstract does not require dismissal of the indictment. When sufficiently coordinated with the FTO, otherwise protected speech can violated Section 2339B.

The defendant next offers the conclusory assertion that his actions "do not clearly fall under the definition of 'service.'" But his argument is contradicted by *HLP*. While the term "service" is not specifically defined in the statute, contrary to the defendant's position, the ordinary meaning of the word suffices. Service is not ambiguous and "does not require similarly untethered, subjective judgments." *HLP*, 561 U.S. at 21. "[A] person of ordinary intelligence would understand the term 'service' to cover advocacy performed in coordination with, or at the direction of, a foreign terrorist organization." *Id.* at 24. Here, the defendant is charged with just that: advocacy performed in coordination with, or at the direction of, ISIS.

With this precedent in mind, the argument that an alleged ambiguity of the "services" in the statute "gives rise to the possibility of discriminatory enforcement"

fails. Br. at 8. "The void-for-vagueness doctrine requires that a penal statute define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited and in a manner that does not encourage arbitrary and discriminatory enforcement." *Kolender v. Lawson*, 461 U.S. 352, 357 (1983). The Supreme Court already has found that Section 2339B meets this threshold.

The defendant's remaining arguments go to the sufficiency of the government's evidence, which present questions for the fact finder at trial, not grounds to dismiss the indictment. "A motion to dismiss is not intended to be a summary trial of the evidence. Such a motion is directed only to the validity of the indictment or the information, and it tests only whether an offense has been sufficiently charged." *United States v. Yasak*, 884 F.2d 996, 1001 (7th Cir. 1989) (internal citation and quote marks omitted); *United States v. Antonucci*, 663 F. Supp. 245, 246 (N.D. Ill. 1987) ("Fed. R. Civ. P. 12(b) was not intended to convert motions to dismiss into a criminal case analogy of the civil practice motion for summary judgment."). Here, the indictment contains the elements of the offense charged, fairly informs defendant of the charge, and enables him to plead an acquittal or conviction in bar of future prosecutions for the same offense. *Hamling*, 418 U.S. at 117 (citations omitted). The defendant does not argue otherwise.

To the extent the defendant wishes to argue that his conduct was protected speech, and that the government has failed to meet its burden to prove the elements of the charges, he may do so at trial. The government alleges that the defendant conspired with other members of Khattab to, at the direction of ISIS, create and

disseminate threats, recruit ISIS supporters, and otherwise distribute ISIS propaganda. The defendant gained unauthorized access to multiple Twitter accounts which he used to promote ISIS and its interests. The defendant argues that writing essays and posting items on Twitter is "pure political speech" and "protected speech". Br. at 11-13. He also claims that he did not act in coordination with ISIS "whatsoever" and that the alleged services lacked value to ISIS. However, these "attack[s] on the factual content of the indictment" provide no grounds for dismissal. *United States v. Ristik*, 2023 WL 2525361, at *2 (N.D. Ill. Mar. 15, 2023) (denying motion to dismiss, which "tests only whether an offense has been sufficiently charged," and "is not intended to be a 'summary trial of the evidence.'").

The defendant's remaining challenges are unsupported. The defendant's suggestions that the material support counts should be dismissed because they do not allege "expert advice or assistance" is inconsistent with the plain language of the statute. The statute specifies "services" as one means by which material support can be provided. The government need not allege additional forms of material support, and defendant provides no contrary authority.

IV. DEFENDANT'S MOTION TO DISMISS COUNT TWO

Count Two alleges that the defendant and members of Khattab conspired to send threats in interstate commerce in violation of 18 U.S.C. § 371. Khattab's messages were designed to "spread terror," "terrorize" and "spread fear" among ISIS's enemies, stating, for example, that the recipients "will not enjoy or dream of safety as long as their governments are fighting the Islamic State." R. 161 ¶8. The targets of Khattab's messages included westerners, Christians and other groups perceived to

be enemies of ISIS. *Id.* The allegations contain a plain, concise, and definite written statement of the essential facts constituting the offense and are sufficient to put defendant on notice of the allegations. *McLeczynsky*, 296 F.3d at 636.

The defendant's arguments for dismissal are unavailing. He alleges that both the conspiracy statute, 18 U.S.C. 371,[1] and the interstate threat statute, 18 U.S.C. 875(c), are unconstitutionally vague as applied because the government does not allege that the defendant personally authored or sent a threat and because the recipient of the threat is not specific enough. He also alleges that no "true threats" were communicated. The first two arguments fail because neither challenged statute is unconstitutionally vague and because defendant's argument misunderstands the elements of the conspiracy charge. Moreover, the defendant's argument that no "true threats" were communicated is, in any event, a factual question properly resolved at trial.

The defendant posits that to be convicted of conspiracy to send threats in interstate commerce, the government must prove that the defendant himself sent a threat. Br. at 19. The defendant misunderstands the law of conspiracy. At trial, the government must prove that the defendant knowingly became a member of the conspiracy with an intent to advance the conspiracy and that one of the conspirators committed an overt act to advance the goals of the conspiracy. Seventh Circuit

[1] The defendant's brief refers to 18 U.S.C. 871, which prohibits threats against the President. The government interprets defendant's motion to refer to Section 371, the conspiracy statute under which he is charged.

Pattern 5.08(A)[2]. These elements are well-established. The government has alleged that the defendant and Co-conspirators A, B, C, and D conspired with others to transmit threats in interstate commerce and identifies a series of overt acts committed to accomplish the objectives of the conspiracy. This is sufficient at the pleading stage. The defendant may argue at trial defendant did not personally author a threat or send a threat. But these factual challenges provide no basis for dismissal.

Next the defendant appears to argue that for the government to prevail on the charge of conspiracy to send threats in interstate commerce, it must prove that a threat was directed as a "specific person or persons." Br. at 21. The defendant is wrong. In *United States v. Khan*, defendant appealed the district court's denial of a motion to dismiss. *United States v. Khan*, 937 F.3d 1042, 1046 (7th Cir. 2019). The indictment charged Khan with sending threats to "kill," "shoot," "hunt," "murder," and "put bullets in" his "targets." The defendant's "targets" included "college student[s]," "vulnerable individuals," people "walking their dogs," "high net worth individual[s]," and "witnesses" that "get [in] the way." *Id.* The district court denied his motion because it presented "a defense relating to the strength of the government's evidence [which] ordinarily must wait for trial." *Id.* at 1049. The Seventh circuit affirmed. *Id.* at 1050.

The Seventh Circuit also rejected the defendant's argument that the government failed to prove the targets of the alleged threats, finding that the defendant's references to "college students, people walking their dogs, truckers, and

[2] The defendant's hypothetical questions about *mens rea* requirement for a conspiracy charge is answered by the Pattern Instruction. *See* Br. at 20.

anyone else who happened to be in the wrong place (Khan's defined "free kill zone") at the wrong time" to be "quite clear." *Khan*, 937 F.3d at 1055. The indictment here alleges that Khattab targeted citizens of citizens of different countries (e.g., the United States, the United Kingdom, France, Australia, Russia and Iraq), Christians (referred to as Cross-worshippers), nations "targeted by the [Islamic] State," and other "disbelievers" or enemies of ISIS. R. 161 ¶ 8. The indictment alleges that the conspiracy involved agreements to send threats to injure for the purpose of "terrorizing" ISIS's enemies and referencing mass attacks like the 2017 Las Vegas shooting. The indictment cites several specific Khattab publications, including one stating, "We will water the earth with your blood. Prepare your coffins. And dig your graves." R. 161 ¶8. These allegations "sufficiently apprised [defendant] of the charges against him in order to enable adequate trial preparation." *Khan*, 937 F.3d at 1049.

Next the defendant argues that the government has not identified anyone who saw one of the videos identified in the indictment. Br. at 21. This is not an element of the charged conspiracy. However, the government's trial evidence will show that these messages were disseminated widely on social media and were reported on by terrorist monitoring organizations. Regardless, to the extent the defendant wishes to argue this, it is another factual issue to dispute at trial.

Because the indictment meets the requirements for putting the defendant on notice of the charges, his motion to dismiss must be denied. Should the defendant wish to challenge the sufficiency of the evidence, he can do so at trial.

V. DEFENDANT'S MOTION TO DISMISS COUNTS 3, 4, 6, 8 AND 10 (TWITTER NOT A PROTECTED COMPUTER)

The indictment alleges that the defendant conspired with others to gain unauthorized access to protected computers and that defendant gained such access through his use of specific Twitter accounts. The indictment properly sets out the elements of the charges and is sufficient to put defendant on notice. The defendant's arguments that Section1030 is impermissibly vague ignores the plain language of the statute. His remaining arguments raise factual questions to be decided at trial. The motion should be denied.

A. Background

The indictment alleges that the defendant conspired to gain unauthorized access to computers through Twitter accounts (Count 3) and intentionally gained unauthorized access to computers, and "thereby obtained information from a protected computer, through [Twitter Accounts A, B, C and D]" in furtherance of a violation Section 2339B(a)(1). (Count Four, Six, Eight, and Ten).

At trial, the government will introduce evidence that the defendant exploited a weakness related to Hotmail accounts that permitted him to reset Twitter account passwords without the account owners' authorization, thus allowing him to take over the Twitter accounts. Those accounts were housed on Twitter's servers, which the evidence will show, are computers located outside the state of Illinois and which are connected to the internet to service accounts in a variety of locations around the world. As alleged, through this Hotmail exploitation, the defendant and other

members of Khattab obtained "hacked" Twitter accounts – accounts accessed without the owner's permission – that they then used to post pro-ISIS information online.

At trial the evidence will show that the defendant saved a copy of a video containing specific instructions on how to gain unauthorized access to Twitter accounts using deactivated Hotmail accounts, and that defendant used that technique to gain unauthorized access to the accounts identified in the indictment.

The defendant has had discovery related to these charges for several years, including search warrant returns from Twitter and Hotmail, records from the defendant's phone (including account login information and numbers of followers for targeted accounts), and a video from defendant's computer containing instructions on how to use Hotmail accounts to get unauthorized access to Twitter account.

B. Argument

The indictment sufficiently alleges the elements of the charged crimes consistent with Rule 7. The defendant's complaints about the alleged vagueness of the indictment and the charged statutes are unfounded.

First, the definition of "computer" in the CFAA is not unconstitutionally vague. *See* Br. at 28. The CFAA defines "computer" as a "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device." 18 U.S.C.A. § 1030(e)(1). It defines a "protected computer" as, among other things, "a computer ... which is used

in or affecting interstate or foreign commerce or communication." 18 U.S.C. §§ 1030(e)(2).

The defendant's concern that the CFAA was written "over twenty years before Twitter was invented" is of no moment. The criminal code need not be amended each time a new technology is invented. The defendant complains that as time has passed, more technology fits into this definition and the ubiquity of social media increases the possibility of "hacking," i.e. gaining unauthorized access to, computers also increases. Br at 28-29. Contrary to the defendant's argument, the fact that more computers exist today than in the past, does not render the terms of the statute unconstitutionally vague.

The allegations of unauthorized access to a protected computer are not impermissibly vague as-applied. The defendant repeatedly asserts that Twitter accounts are not computers. *E.g.* Br. at 33. This argument misstates the allegations. The indictment alleges that the defendant accessed protected computers through Twitter accounts: namely, by accessing these social media accounts, he accessed Twitter's servers. Servers plainly qualify as "high speed data processing devices" which are "used in or affecting interstate or foreign commerce." Indeed, servers fall under the most basic and readily understandable definition of computer. A "server is a computer because it is a 'data processing device'… That's the whole point of a server – processing and retaining data." [3] *ACW Flex Pack LLC v. Wrobel,* No. 22-cv-6858,

[3] Defendant lists several devices through which Twitter accounts can be accessed, such as tablets and mobile phones. Br. at 35. These examples are irrelevant to the accounts' necessary connection to hosting servers operated by Twitter.

2023 WL 4762596, at *7 (N.D. Ill. July 26, 2023) (holding that "[s]ervers fit within the plain language" of the CFAA); *see also, Sell It Soc., LLC v. Strauss,* 2018 WL 2357261, at *2 (S.D.N.Y. Mar. 8, 2018) (where the victim "housed the database on servers, a data storage facility, and [defendant] accessed those servers to download the database, [defendant] accessed a computer. …That computer is also a 'protected computer' because it is used in interstate commerce"); *Paradigm Alliance, Inc. v. Celeritas Technologies*, LLC, 248 F.R.D. 598, 602 (D. Kan. 2008) ("As a practical matter, a computer providing a 'web-based' application accessible through the internet would satisfy the 'interstate communication' requirement.").

In addition, the Twitter accounts themselves are "communications facility[ies] directly related to or operating in conjunction with" those servers, consistent with the definition of computer in Section 1030(e)(1). "Consistent with the plain language of the statute, most courts hold that unauthorized access to web-based accounts can form the basis of a CFAA violation[.]" *Hill v. Lynn*, 2018 WL 2933636, at *3 (N.D. Ill. June 12, 2018). *See also, Taylor Made Express, Inc. v. Kidd*, 2024 WL 197231, at *8 (N.D. Ill. Jan. 18, 2024) (the "Outlook 365 email system is a 'computer' for purposes of the CFAA" because it is a "data storage facility or communications facility directly related to or operating in conjunction with" physical computers.); *Wrobel*, 2023 WL 4762596, at *6 ("ACW has plausibly alleged that by accessing the data on Microsoft's 365 cloud services, defendants accessed a 'computer' as defined by the [CFAA]."); *Feldman v. Comp Trading, LLC*, 2021 WL 930222, at *6 (E.D.N.Y. Mar. 11, 2021) ("the Microsoft 365 cloud server" can support a CFAA claim).

Defendant cites cases consistent with the ones above. *See* Br. at 30 (citing *Hill v. Lynn*, 2018 U.S. Distr. LEXIS 98197 (N.D. Il. 2018) and *United Resin Inc. v. Los*, 2022 U.S. Dist. LEXIS 207991 (E.D. Mi. 2022)). He also cites two cases to the contrary, but they do not support his claims. In *Owen v. Cigna*, 188 F. Supp. 3d 790, 793 (N.D. Ill. 2016), the court examined a civil complaint alleging that plaintiff's former employers accessed the computer she previously used at work without authorization. The allegations in *Owen* were not centered on servers hosting a social media account but rather on whether an employer could access its own computer without authorization. In dismissing the complaint, the court noted that plaintiff failed to allege that she "retained any authority to grant or deny anyone permission to access her former work computer after she left" and "the only computer Owen alleges defendants accessed without authority is her former work computer."

Christie v. Nat'l Inst. For Newman Studies, Br. at 30, dealt with similar questions of unauthorized access in a civil, employment context. 2019 WL 1916204, at *8 (D.N.J. Apr. 30, 2019). There, plaintiff, a former employee, alleged that defendants accessed their own company computers without plaintiff's authorization. The court found that "Plaintiff cannot, as a legal matter, exert control" over the work computers defendant allegedly accessed because defendant was "the rightful owner of those machines." *Id.* To the extent emails were accessed, the court cited expert testimony that defendant "could view e-mails sent or received using the …e-mail account without accessing the remote server by accessing copies *already stored locally*

on the ...desktop." *Id.* (emphasis added). In short, the email access was not tied to the email providers' storage.

The defendant next turns to the term "unauthorized access," arguing, yet again, that it is impermissibly vague. *See* Br. at 31. It is not. The Second Circuit analyzed the term authorization as used in the CFAA, holding that "authorization" is a word "of common usage, without any technical or ambiguous meaning." *United States v. Valle*, 807 F.3d 508, 524 (2d Cir. 2015) (*citing United States v. Morris*, 928 F.2d 504, 511 (2d Cir.1991). The court noted that the dictionary defines "authorization" as "permission or power granted by authority." *Id.* And "common usage" "suggests that one 'accesses a computer without authorization' if he accesses a computer without permission to do so at all.") *Id*. The same common usage principles apply here. As alleged, the defendant accessed Twitter accounts without permission to do so at all. This is sufficient at the pleading stage.

The various hypotheticals offered by the defendant do not require any different finding. In *United States v. Singla*, 2023 WL 5938082, at *8 (N.D. Ga. Sept. 12, 2023), the court held that the indictment alleging that defendant accessed a protected computer at a medical center and obtained information from it was not unconstitutionally vague as to the defendant. The court distinguished the same type of hypothetical questions presented here, noting that while "there may be some hypothetical cases where § 1030(a)(2)(C) is harder to apply does not mean the provision is unconstitutionally vague as applied to [defendant]. The indictment properly alleges the defendant committed acts that § 1030(a)(2)(C) clearly makes

criminal—that is, that he intentionally accessed without authorization…" protected computers. *Id.* at *8 (N.D. Ga. Sept. 12, 2023).

Next, the defendant argues that there is no "information" to be obtained from Twitter accounts. Br. at 25. This statement misunderstands the statute and the nature of social media. The term "obtaining information" is an expansive one that includes *merely viewing information without downloading or copying a file*. *See* S. Rep. No. 99-432, at 6 (emphasis added); *see also, America Online, Inc. v. National Health Care Discount, Inc.*, 121 F. Supp. 2d 1255, 1275 (N.D. Iowa 2000). Information stored electronically can be obtained not only by actual physical theft, but also by "*mere observation of the data*." *Id.* (emphasis added).

In addition to the legal sufficiency of the allegations, the defendant's argument fails because he again seeks to have the court make factual determinations prior to trial. But there is no summary judgment in criminal cases. Instead, the defendant may challenge the government's proof at trial. Here, the government's evidence will show that by logging in to Twitter accounts owned and created by others without their permission, the defendant obtained information.[4] This information includes information accessible in the account login portal, the content of previous posts by the true account holder, and the numbers of followers for the accounts, among other items. Additionally, by accessing the accounts, the defendant viewed and altered

[4] The defendant is correct that, in addition to obtaining information, the indictment alleges that defendant used his access to protected computers, via Twitter accounts, to share information. S*ee* Br. at 25. This does not support dismissal; on the contrary, it is relevant to the allegation that the unauthorized access was in furtherance of the Section 2339B violations. The evidence will show that the accounts were used to promote ISIS.

account settings, notably, password information. Indeed, the evidence will show that defendant not only obtained information by viewing contents of the accounts, but he also extracted information about the accounts, including login credentials and numbers of followers, and recorded that information on his phone. In addition, by accessing the accounts, the defendant caused Twitter to send information to email addresses he controlled related to those accounts. Accordingly, the indictment sufficiently alleges that the defendant "obtained information" under the statute. *United States v. Drew*, 259 F.R.D. 449, 457 (C.D. Cal. 2009) (denying Rule 29 motion because "Obtain [ing] information from a computer" has been described as "'includ[ing] mere observation of the data. Actual aspiration ... need not be proved in order to establish a violation....'). The defendant's factual challenges must await trial.

The defendant's remaining arguments also turn on a factual question: was the access to Twitter accounts "unauthorized." The defendant's conclusory assertions that the Twitter accounts were "abandoned," and his efforts to organize unauthorized access events into "intended function," "agency relationship" and "contract breach" approaches amount to factual arguments to be decided by at trial. See Br. at 37. Indeed, he cites no authority for dismissal of any indictment on such grounds. His motion should be denied.

VI. DEFENDANT'S MOTION TO QUASH SEARCH WARRANT

On October 16, 2018, the government applied for, and was issued, a warrant to search the defendant's home and various electronic devices located within (Warrant attached as Exhibit A). The defendant argues that warrant should be suppressed because, first, the "crimes' alleged were 100% protected by the First

Amendment," and, second, because the warrant was not supported by probable cause. Br. at 41-45. The defendant is incorrect on both counts. The criminal acts alleged in the affidavit—e.g. coordinated activity with ISIS to create and distribute propaganda to recruit for and encourage attacks in support of same, among other offenses—are not protected First Amendment activities. Moreover, the warrant was supported by ample probable cause, including, among other evidence, numerous recorded online communications in which the defendant helped coordinate media campaigns on behalf of ISIS for Khattab, implemented directions provided by ISIS, managed other Khattab writers as head of the Khattab Writers Group, drafted and published ISIS propaganda, and worked to publish ISIS propaganda through various social media channels online. Additionally, even if the Court were to find that the warrant issued without probable cause, it still should not be suppressed because the agents relied in good faith on its issuance by the magistrate.

With respect to the defendant's first argument, that the underlying criminal acts supporting the issuance of the warrant were protected First Amendment activities, consistent with the Supreme Court's holding in *HLP*, the Seventh Circuit has explained, "The right to free speech, religious and political expression, and association are limited by Congress's authority to prohibit expressive activity that amounts to the provision of material support to a foreign terrorist organization where the support is either addressed to, directed by, or coordinated with that organization." *Osadzinski*, 97 F.4th at 492 (internal quotation marks omitted) (affirming defendant's Section 2339B conviction).

The warrant affidavit in question here alleged similar activities: namely, that defendant worked with other members of Khattab "at the direction of and in coordination with ISIS and ISIS's media office" to create and disseminate ISIS propaganda, recruit for ISIS, encourage individuals to carry out attacks on behalf of ISIS, and support violent jihad on behalf of ISIS. In other words, precisely the type of activities that the Seventh Circuit held beyond the protection of the First Amendment in *Osadzinski*. *See also HLP*, 561 U.S. 1 (distinguishing "independent advocacy," which is protected by the First Amendment, from "advocacy performed in coordination with, or at the direction of, a foreign terrorist organization," which is not).

The defendant's claim that the warrant issued without probable cause is equally unavailing. As the Seventh Circuit has explained, "Probable cause is established whenever there is a reasonable probability of finding the desired items in a particular location." *United States v. Rambis*, 686 F.2d 620, 622 (7th Cir.1982). This requires no more than "a fair probability that contraband or evidence of a crime will be found in a particular place." *United States v. Gibson*, 996 F.3d 451, 461 (7th Cir. 2021). "[A] magistrate's determination of probable cause is to be given considerable weight and should be overruled only when the supporting affidavit, read as a whole in a realistic and common-sense manner, does not allege specific facts and circumstances from which the magistrate could reasonably conclude that the items sought to be seized are associated with the crime and located in the place indicated." *United States v. Pritchard*, 745 F.2d 1112, 1120 (7th Cir. 1984).

The defendant's argument that the October 16, 2018, warrant lacked probable cause is largely premised on his gross mischaracterization of the evidence. The defendant's Motion focuses on only two facts from the affidavit: defendant's use of a VPN, and his deletion of data from his own devices. Br. at 41-45. The defendant argues that because there could be innocent explanations for these two pieces of information, they cannot support probable cause, and therefore the warrant should be suppressed. As an initial matter, the defendant is incorrect that these two facts cannot support probable cause, irrespective of whether an innocent explanation might also exist. *United States v. Gary*, 790 F.3d 704, 707–08 (7th Cir. 2015) (probable cause exists even though there "could have been innocent explanations" for the targeted activity, so long as "the inference of the criminal activity was reasonable"). In any event, the two facts highlighted by the defendant are only a small segment of the evidence described in the warrant and its attachment.

As described in the affidavit, beginning around 2017, an FBI Undercover Employee captured numerous online communications between Khattab members, including the defendant. Those communications revealed that the defendant and his fellow Khattab members were working in coordination with ISIS and ISIS's media office to create and distribute propaganda designed to encourage others to join ISIS and carry out attacks on its behalf. Among other things:

- The purpose of Khattab was to create and disseminate propaganda on behalf of ISIS in the form of images, articles, and videos meant to spread fear and recruit for the terrorist group. Ex. A, at 39-51.

- Khattab's rules provided that members, acting at the direction and control of ISIS and ISIS' media office, had to disseminate only information supportive of ISIS. *Id.* at 46-49.

- The defendant was an active member of Khattab and later the head of its Writers Group. *Id.* at 51-52.

- Between October 2017 and December 2017, Khattab considered merging with another ISIS propaganda group, but abandoned the merger at ISIS's direction. Id. at 47-49.

- In November 2017, the defendant encouraged other Khattab members to help ISIS in any way possible, including by offering money or their lives. *Id.* at 43.

- In December 2017, the defendant encouraged other Khattab members to spread ISIS's message as widely as possible on social media. *Id.* at 45.

- In March 2018, the defendant reposted an admonishment to other Khattab members that they must adhere to ISIS's official media statements and act in accordance with ISIS's instructions. *Id.* at 47.

- The defendant's pledged allegiance to Abu Bakr Al-Baghdadi, the leader of ISIS in March 2018. *Id.* at 41-42.

- In May 2018, the defendant instructed his fellow Khattab members to "[p]articipate in the war, and spread fear . . . [t]he Islamic State doesn't want you to watch these publications only, rather [ISIS] wants to mobilize you." *Id.* at 45.

- In June 2018, the defendant and other Khattab members discussed and shared methods of hacking into the social media accounts of legitimate users to publish ISIS propaganda. *Id.* at 63-70.

The affidavit contains several examples of Khattab's work, including videos glorifying death in battle on behalf of ISIS, a video threatening an impending attack, and a video posted by the defendant threatening the Egyptian people to stay away from polling stations during the March 2018 presidential election. *Id.* at 52-56. The affidavit contains examples of pro-ISIS infographics published by Khattab, and an

article written by the defendant for Khattab that praise ISIS and jihad. *Id.* at 56-62. The affidavit additionally contains evidence tying the defendant to the residence and establishing his use of electronic devices to conduct Khattab propaganda activities. *Id.* at 5-15.

As such, the defendant's claim that "the only evidence presented [in the warrant] was Mr. Safoo's legal attempts to protect his privacy" is flatly wrong. Rather, the affidavit contains ample evidence establishing the defendant's involvement with Khattab, Khattab's connection with ISIS, the defendant's efforts to provide support to ISIS via his work for Khattab, and the probable cause for believing that evidence of these offenses would be located in the defendant's residence and devices.

Even assuming, arguendo, that a Fourth Amendment violation had occurred, suppression would be inappropriate because law enforcement officers relied in good faith on the issuance of the warrant by the Magistrate. As is the case here, an "officer's decision to obtain a warrant is prima facie evidence of good faith," *United States v. Woolsey*, 535 F.3d 540, 546 (7th Cir. 2008), and the defendant bears the "heavy" burden to rebut that presumption. *United States v. Matthews*, 12 F.4th 647, 653 (7th Cir. 2021).

The defendant has not attempted to do so in his motion, nor could he do so successfully. To meet this "heavy burden," the defendant must establish one of four things: (1) the application's affiant misled the issuing judge with information that "the affiant knew was false or would have known was false but for the affiant's

reckless disregard for the truth"; (2) the issuing judge "wholly abandoned his judicial role and instead acted as an adjunct law-enforcement officer"; (3) the affidavit so lacked "indicia of probable cause as to render official belief in its existence entirely unreasonable"; or (4) the warrant "was so facially deficient in particularizing its scope that the officers could not reasonably presume it was valid." *United States v. Rees*, 957 F.3d 761, 771 (7th Cir. 2020).

Here, the defendant has not argued that the affiant to the warrant misled the magistrate, nor that the magistrate "wholly abandoned his judicial role," nor that the warrant was facially deficient in particularizing its scope. To the extent the defendant intended to argue that the warrant so lacked probable cause as to render official belief in its existence unreasonable, his argument lacks merit. As described above, the warrant contained more than adequate probable cause to support its issuance. As such, even if the defendant were correct—and he is not—that the warrant was not supported by probable cause, there would still be no suppression remedy available in this instance because the officers relied in good faith on the issuance of the warrant by the magistrate.

VII. MOTION TO SUPPRESS EVIDENCE

The defendant next argues that, based on the Supreme Court's decision in *United States v. Carpenter*, 138 S. Ct. 2206 (2018), the Court should suppress all evidence obtained pursuant to the Stored Communications Act ("SCA"). The argument is without merit.

In *Carpenter*, the Supreme Court held that "[g]iven the unique nature of cell phone location records . . . an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through [cell-site location information]," regardless of whether the information was revealed to the cell-phone company. *Id.* at 2217. The Supreme Court emphasized the "special solicitude for location information in the third-party context" because such information provides "an all-encompassing record of the holder's whereabouts," which placed cell-site location information in a "qualitatively different category" than "telephone numbers and bank records." *Id.* at 2216-19. The Supreme Court explicitly stated that their decision in Carpenter was a "narrow one," limited to some cell-site records. *Id.* at 2220. It explained it was not disturbing the third-party doctrine created by *Smith* and *Miller*—the cases that held business records and other information revealed to a third party receive no Fourth Amendment protection. *See id.*

Despite the clear language limiting the applicability of *Carpenter* to some cell-site location information, the defendant argues that the Court should extend the decision to impose a warrant requirement on the collection of seemingly all digital evidence under the SCA. Br. at 45-62. Notably, it is not clear from the defendant's motion what records in particular he is seeking to suppress. The defendant refers to his Attachment 1 at several points, but Attachment 1 appears to contain a list various items of evidence produced in the case, including records obtained via warrant or other non-SCA process, along with what seem to be personal reflections on the content and volume of the materials.

Assuming the defendant is seeking to suppress all SCA process, there is no basis to do so under *Carpenter* or its progeny. The Fourth Amendment does not apply to the information collected because of the third-party doctrine. All the information at issue—subscriber information, financial records, toll records, IP records, etc.—was voluntarily disclosed to the third-party businesses by the defendant or some other entity. Because the information had already been disclosed, the defendant did not have an objectively reasonable expectation of privacy in this information. As a result, the Fourth Amendment does not protect the information and no suppression remedy is available. *See United States v. Miller*, 425 U.S. 435, 441-42 (1976) (no reasonable expectation of privacy in a customer's bank records); *Smith v. Maryland*, 442 U.S. 735, 741-42 (1979) (no reasonable expectation of privacy in numbers dialed); *Huon v. Mudge*, 597 F. App'x 868, 875 (7th Cir. 2015) (no reasonable expectation of privacy in user's subscriber information or the numbers dialed); *United States v. Caira*, 833 F.3d 803, 809 (7th Cir. 2018) (no reasonable expectation of privacy in a user's Internet protocol (IP) connection records).

Carpenter did not alter this analysis. As noted, Carpenter was a "narrow" holding, applicable only to the warrantless collection of cell-site location information, and which did not otherwise alter the third-party doctrine. Thus, every Circuit, including the Seventh Circuit, that has considered the extension of Carpenter to other non-content records—such as subscriber information, toll records, IP addresses, etc.—has declined to do so. *See, e.g.*, *United States v. Mitrovich*, 95 F.4th 1064, 1068 (7th Cir. 2024) ("[O]ur precedent . . . established that a person has no reasonable

expectation of privacy in their IP address because they voluntarily share it with third parties while browsing the internet"); *United States v. Soybel*, 13 F.4th 584, 592 (7th Cir. 2021) ("Soybel contends that after *Carpenter* he has a reasonable expectation of privacy in his personal [i]nternet traffic data. We disagree. As three of our sister circuits have recognized, *Carpenter* has no bearing on the government's collection of IP-address data from a suspect's internet traffic"); *United States v. Trader*, 981 F.3d 961, 968 (11th Cir. 2020) ("[E]very circuit to consider the question [about subscriber information and IP addresses] after Carpenter has reached the same conclusion" that the information remains unprotected by the Fourth Amendment); *United States v. Morel*, 922 F.3d 1, 8 (1st Cir. 2019) ("IP address information of the kind and amount collected here – gathered from an internet company – simply does not give rise to the concerns identified in *Carpenter*."); *United States v. Contreras*, 905 F.3d 853, 857 (5th Cir. 2018) (declining to extend *Carpenter* to logging of IP address in website's records because "[t]hey had no bearing on any person's day-to-day movement"); *United States v. Whipple*, 92 F.4th 605, 611–12 (6th Cir. 2024) (explaining that the Court in *Carpenter* "was careful not to disturb the application of the traditional third-party doctrine to voluntary disclosures" and thus "[t]he Government will be able to use subpoenas to acquire records in the overwhelming majority of investigations") (quoting *Carpenter*, 138 S. Ct. at 2222); *United States v. Rosenow*, 50 F.4th 715, 738 (9th Cir. 2022) (explaining that Carpenter did not change the fact that 'a defendant "ha[s] no expectation of privacy in ... IP addresses" or basic subscriber information because internet users "should know that this information is provided to and used by

Internet service providers for the specific purpose of directing the routing of information") (quoting *United States. v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008)); *States v. Wellbeloved-Stone*, No. 18-4573, 4 (4th Cir. Jun. 13, 2019) (post-Carpenter, defendant still "had no reasonable expectation of privacy in his subscriber information, and the Government did not perform a Fourth Amendment search by obtaining that information"); *see also United States v. Barnett*, No. 17-CR-00676, 2023 WL 1928202, at *16 (N.D. Ill. Feb. 10, 2023) (no expectation of privacy under *Carpenter* in IP address information generated by defendant's mobile device); *United States v. Ji*, No. 18 CR 611, 2021 WL 5321046, at *1 (N.D. Ill. Nov. 16, 2021) (holding that Carpenter did not create an expectation of privacy in subscriber information, IP information, telephone numbers, financial records, or other similar non-content records because such records do "not provide the same all-encompassing record of Ji's whereabouts that CSLI would have" and the defendant assumed the risk by voluntarily communicating with third parties").

Even if a Court were to find that warrantless gathering of this information somehow violated the Fourth Amendment, there still would be no suppression remedy because the FBI relied in good faith on the SCA when it gathered the information. Courts have long held that where law enforcement relies on a statute to gather information without a warrant, the evidence cannot later be suppressed even if a court rules a warrant was required. *See, e.g., Illinois v. Krull*, 480 U.S. 340 (1987) (holding the Fourth Amendment's exclusionary rule does not apply to evidence obtained by police who acted in objectively reasonable reliance upon statute

authorizing warrantless administrative searches, but which was subsequently found to violate Fourth Amendment); *United States v. Hammond*, 996 F.3d 374 (7th Cir. 2021) (no exclusionary rule where officers relied on the SCA to gather information without a warrant); *Soybel*, 13 F.4th at 592–94 (7th Cir. 2021) (suppression is not the proper remedy for "evidence seized pursuant to a statute subsequently declared unconstitutional.")

The non-content records the government obtained in this case were not cell site records. They were basic information such as the defendant's name and address, call records, and summary information about his usage of various services. The information collected falls within the core of the third-party doctrine and therefore the information cannot be suppressed pursuant to the Fourth Amendment. The defendant's argument, if accepted, would dramatically alter the scope of the Fourth Amendment and effectively invalidate the SCA, which expressly provides a mechanism for the government to obtain basic subscriber data. *Carpenter* did not usher in this massive change when the Supreme Court explicitly stressed that its decision was a narrow one.

Lastly, the defendant points to questions posed by Justice Gorsuch in a dissent in *Carpenter* in which the Justice suggested that property law, including the law of bailments, could hypothetically justify the protection of data contractually entrusted to third parties. The defendant asks that the Court use this dissent as a basis to invalidate any "clickwrap" Terms of Services agreements which might be applicable to the information obtained by the government. The defendant alternatively requests

that the Court hold that any information provided by defendant to third-party providers is in fact an involuntary bailment and that the third-party providers therefore stole it when they turned it over to the government.

In particular, the defendant asks the Court to "hold that Silicon Valley [Terms of Service] agreements are not contracts, and their terms are not enforceable." Although it is not expressly clear from his Motion, presumably the defendant intends to argue that, after broadly invalidating the 'Silicon Valley' terms of services agreements that might be applicable to the information obtained by the government from third-party providers via the SCA, the Court should next hold that the absence of such enforceable agreements renders the third-party doctrine inapplicable and makes the acquisition of that data a search. Although various Terms of Service agreements no doubt applied to much of the content at issue in this case, the defendant has not identified a single one, let alone explained why the terms of any particular agreement made it a "clickwrap" agreement, nor why or under what authority this Court would invalidate any particular agreement between defendant and a non-party third-party provider, nor how invalidating that agreement would require the suppression of any evidence obtained from that third-party provider.

Instead, the defendant asks the Court to take the extraordinary step of holding that any hypothetically relevant "Silicon Valley [Terms of Services] agreements are not contracts," and then take the even more extraordinary step—supported by no legal authority—of holding that in the absence of enforceable Terms of Services agreements, evidence obtained from third-party providers via the Stored

Communications Act should be suppressed. Alternatively, the defendant asks that the Court hold that defendant had entered into bailments with the third-party providers to whom he voluntarily provided his information. The defendant requests—again citing no supportive legal authority and offering no factual specifics—that the Court hold that these providers in fact *stole* defendant's property when they provided it to the government in response to valid legal process. The Court should decline the invitation.

VIII. CONCLUSION

For the reasons set forth above, the government requests that the Court deny defendant's pretrial motions.

Respectfully submitted,

MORRIS PASQUAL
Acting United States Attorney

By: /s/ *Barry Jonas*
BARRY JONAS
MELODY WELLS
A.J. DIXON
Assistant United States Attorneys
219 South Dearborn Street, 5th Floor
Chicago, Illinois 60604

Dated: May 30, 2024