

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION**

UNITED STATES OF AMERICA,

Plaintiff,

v.

ASHRAF AL SAFOO.

Defendant.

Case No. 18 CR 696

Judge John Robert Blakey

MEMORANDUM OPINION AND ORDER

On March 12, 2020, Defendant was charged by a Second Superseding Indictment (“the indictment”) with: conspiracy to provide material support to a foreign terrorist organization, in violation of 18 U.S.C. § 2339B(a)(1); conspiracy to transmit threats in interstate commerce, in violation of 18 U.S.C. § 371; conspiracy to intentionally access a protected computer without authorization, in violation of 18 U.S.C. § 371; multiple counts of intentionally accessing a protected computer without authorization, in violation of 18 U.S.C. § 1030(a)(2) and (c)(2)(B)(iii); and multiple counts of providing material support to a foreign terrorist organization, in violation of 18 U.S.C. § 2339B(a)(1). [161].

Pending before the Court are Defendant’s pretrial motion for a bill of particulars [339], motions to dismiss on multiplicity grounds [340] [341], and untimely omnibus motion to dismiss and suppress [372], and the government’s *Santiago* motions, [305] and [377]. This Court permitted full briefing on all motions, [339], [340], [341], [345], [372], [389], and [393], and held oral argument on June 25, 2024. Having considered the parties’ oral and written arguments, the Court resolves all motions below.

I. Defendant’s Motion for a Bill of Particulars [339]

Defendant moves under Federal Rule of Criminal Procedure Rule 7(f) for a bill of particulars, requesting an order directing the government to identify: (1) the “specific identities” and “known aliases” of the members of the conspiracy charged in Counts 1–3; (2) the “communications containing threats” alleged in Count 2; (3) all “material support,” “resources” and “services” charged in Counts 5, 7, 9, and 11; and

(4) all “protected computers” accessed and “information” obtained, charged in Counts 4, 6, 8, and 10. [339] at 11–13.¹ The Court addressed these requests in turn below.

The decision to order a bill of particulars “rests within the sound discretion of the district court.” *United States v. Hernandez*, 330 F.3d 964, 975 (7th Cir. 2003). A bill of particulars provides a “more specific expression” of the illegal conduct for which defendant is accused, *United States v. Canino*, 949 F.2d 928, 949 (7th Cir. 1991), and thus enables a defendant to prepare an adequate defense. *See United States v. Kendall*, 665 F.2d 126, 134 (7th Cir. 1981). A defendant “is not entitled to know all the evidence the government intends to produce, only the theory of the government’s case.” *Id.* at 34. (internal quotations omitted).

In assessing the need for a bill of particulars, the “key question is whether the defendant was sufficiently apprised of the charges against him in order to enable adequate trial preparation.” *United States v. Vaughn*, 722 F.3d 918, 927 (7th Cir. 2013) (quoting *United States v. Blanchard*, 542 F.3d 1133, 1140 (7th Cir. 2008)). An indictment is sufficient, and a bill of particulars unnecessary, if the indictment “includes each of the elements of the charged offense, the time and place of the accused’s criminal conduct, and a citation to the applicable statute or statutes.” *United States v. Fassnacht*, 332 F.3d 440, 446 (7th Cir. 2003); *Vaughn*, 722 F.3d at 927. Likewise, a bill of particulars is “unnecessary if the information the defendant seeks is readily available through alternative means such as discovery. *Vaughn*, 722 F.3d at 927 (quoting *Blanchard*, 542 F.3d at 1140).

A. Identities of Co-Conspirators

Defendant argues that he requires disclosure of the specific identities and known aliases for Co-Conspirators A, B, C, and D (presently identified by their Twitter “handles”) to confirm that an alleged co-conspirator was not in actuality a government agent. [339] at 6–7.

The government responds that it has already provided, through discovery, information enabling Defendant to identify Co-Conspirators A through D to Defendant, including all of the communications by Khattab Media Foundation (“Khattab”) members in its possession, which identify members by their handle, and thus inform Defendant of their identities. [230] at 4. Further, at the motion hearing held on June 25, 2024, the government agreed to tender information specifically connecting the known Co-Conspirators A through D, as identified in the indictment, to their respective “handles.” As stated in open court, should the government possess and fail to tender any additional identifying information to the Defendant consistent with its discovery obligations, it will not be permitted to present such evidence at

¹ Defendant initially moved for a bill of particulars under former defense counsel, [216], and renewed the original requests in the current motion [339]. The government has rested on its response [230] to Defendant’s original motion for a bill of particulars, *see* [345].

trial. The Court ordered the government to tender this information by July 8, 2024. [396]. Accordingly, the Defendant has received all of the information he seeks on this issue, and the Court therefore denies Defendant's request as moot.

B. Threats

Defendant argues that the government should identify the "threats" alleged in Count 2 so that he can determine whether they are "true threats" and raise any applicable First Amendment defenses. The government responds that Count Two of the indictment outlines "multiple, specific threats," designed to "spread terror," "terrorize" and "spread fear" as outlined in ¶ 8, (a)–(m). The Court agrees with the government.

The indictment sufficiently details the specific threats underlying the charge, the dates of each threat, the means by which the threats were communicated, and a citation to the statute violated. [161], ¶ 8. For example, the indictment states:

On or about December 26, 2017, Khattab created and distributed on the internet a video titled "Our gifts are ready." The video stated "Now listen you dogs of hell. This is a message and more are going to follow. This is just the beginning. Our gifts are now ready." The video shows a present under a Christmas tree that contains a bomb with a timer ticking down before cutting to a video of a mass shooting. The video then uses animation to show families standing around the Christmas tree. Standing behind them is a person dressed in all black and holding what appears to be a detonator. As he raises the detonator, the video flashes to various landmarks and cities, including: Berlin, Brussels, London, Moscow, New York, Paris, and Sydney. The soldier then detonates the bomb and the video is engulfed in flames. The video ends with the Khattab logo.

[161] ¶ 8 (h).

These allegations sufficiently put the Defendant on notice of the charges against him and enable him to prepare an adequate defense. *Fassnacht*, 332 F.3d at 446. Indeed, without a bill of particulars, Defendant has already presented his challenge to Count 2 on First Amendment grounds. *See* [372]. Again, finding no basis to order a bill of particulars, the Court denies Defendant's request.

C. Material Support, Resources, and Services

Defendant argues that the statutory definition of "material support or resources," 18 U.S.C. § 2339A(b)(1) is non-exhaustive and used ambiguously in the indictment, such that the "services" identified in Count 1 may be different than the

“services” identified in Counts 5, 7, 9 and 11. [339] at 8–9. Regarding these counts, Defendant asserts that the meaning of these terms should be clarified so he can make all necessary pretrial motions, including First Amendment challenges to the indictment. *Id.*

It is apparent from the face of the indictment that the “services” identified in Count 1 refer to the same conduct as the “services” in Counts 5, 7, 9, and 11. Count 1 charges Defendant with conspiracy to provide material support and resources to a foreign terrorist organization in violation of 18 U.S.C. § 2339B(a)(1), while Counts 5, 7, 9, and 11 charge Defendant with the underlying substantive violation of § 2339B(a)(1). The indictment alleges that Defendant was a member of Khattab, an “internet-based organization dedicated to the creation and dissemination of pro-ISIS...video content and infographics” which it posted “across multiple social media platforms including Twitter.” [161], Count 1, ¶¶ 6–8. Khattab members created this content and seized Twitter accounts A through D to disseminate this content “on behalf of ISIS using Twitter,” *id.*, Count 3, ¶ 3. And Counts 5, 7, 9, and 11 allege that Defendant “knowingly provided and attempted to provide material support and resources, namely, services through Twitter Account” A through D. *See id.*, Counts 5, 7, 9, and 11, ¶ 2.

As with Count 2, Defendant’s arguments in support of his motion to dismiss [372] reflect this same understanding of “services” as used in the indictment. [372] at 5.² And, again, Defendant has already raised the First Amendment challenges for which he claims the need for a bill of particulars. *See id.* at 12–13. Thus, a bill of particulars is not necessary to accomplish this aim, and the Court denies this request.

D. Protected Computer

Defendant argues that the government should identify with particularity what it means by “protected computer” because it is “entirely unclear what ‘information’ was ‘obtained’ from the protected computers.” [339] at 10. Counts 4, 6, 8, and 10 allege that Defendant “intentionally accessed a protected computer used in interstate and foreign commerce without authorization, and thereby obtained information from

² In support of his motion to dismiss, Defendant states:

In general, the indictment alleges that Mr. Safoo and his Co-conspirators used Hotmail accounts to change the passwords for various Twitter accounts, so that they could perform Twitter “raids”. Counts Five, Seven, Nine and Eleven each detail a specific instance in which Mr. Safoo and his Co-conspirators engaged in a scheme to perform a “Twitter raid.” During these “raids”, the government alleges, Mr. Safoo and his Co-conspirators posted essays and a cartoon propaganda video. Thus, according to the government, the “material support” in question was the “service” of posting those essays and cartoons.

[372] at 5.

a protected computer” through Twitter Accounts A through D. [161], Count 4 ¶ 2, Count 6 ¶ 2, Count 8 ¶ 2, Count 10 ¶ 2.

The government argues that the indictment contains “detailed information” concerning Defendant’s access to Twitter Accounts A through D, including that “Khattab members shared information related to ‘seizing’ or ‘hacking’ social media accounts, including Twitter,” and it further identifies “by date and account, the Twitter accounts that were accessed without authorization.” [230] at 5. The government further contends that it has provided, via the ample discovery tendered in this case, the “documents and information related to these counts, including evidence from defendant’s electronic devices and documents obtained from Twitter and Microsoft.” *Id.* At the motion hearing, the government proffered that this discovery confirms the government’s theory that Defendant accessed a “protected computer”—namely, Twitter’s server(s)—through Twitter accounts A, B, C, and D. For example, the government cited a report from a Twitter representative who is expected to testify regarding Twitter and its servers, and the Defendant acknowledged that he had not yet reviewed that discovery. Such discovery provides sufficient detail to render a bill of particulars unnecessary.

Accordingly, the Court denies Defendant’s motion in its entirety.

II. Defendant’s Motions to Dismiss on Multiplicity Grounds [340] [341]

Defendant moves to dismiss Counts 4, 6, 8, and 10, which charge him with unauthorized access to a protected computer in violation of 18 U.S.C. § 1030(a)(2)(C), and Counts 5, 7, 9, and 11, which charge him with providing material support to a foreign terrorist organization, in violation of 18 U.S.C. § 2339B, on multiplicity grounds. [340] [341].

An indictment is “multiplicitous” if it “charges a single offense as separate counts.” *United States v. Corrigan*, 912 F.3d 422, 427 (7th Cir. 2019) (quoting *United States v. Ajayi*, 808 F.3d 1113, 1123 (7th Cir. 2015)). An indictment is not multiplicitous, however, “merely because it charges more than one violation of the same statute based on related conduct; instead, a defendant can be convicted of multiple violations of the same statute if the conduct underlying each violation involves a separate and distinct act.” *United States v. Chilaca*, 909 F.3d 289, 291–92 (9th Cir. 2018).

Multiplicity can come in two forms. The first type occurs when the “same act or transaction” constitutes a violation of two distinct statutory provisions. *Blockburger v. United States*, 284 U.S. 299, 304 (1932). For that type, the test for multiplicity is “whether each provision requires proof of a fact which the other does not.” *Id.* The second type, at issue here, occurs when “charges for multiple violations of *the same statute* are predicated upon arguably the same criminal conduct.” *United*

States v. Woerner, 7098 F.3d 527, 539 (5th Cir. 2013). For this type, to determine whether an indictment is “multiplicitous,” the Court must assess whether it alleges that “separate and distinct prohibited acts, made punishable by law, have been committed.” *United States v. Naidoo*, 995 F.3d at 380 (5th Cir. 2012) (citing *United States v. Planck*, 493 F.3d 501, 503 (5th Cir. 2007)). The Court looks to the applicable criminal statute to discern the “allowable unit of prosecution”—the minimum amount of activity for which criminal liability attaches.” *United States v. Haas*, 37 F.4th 1256, 1261 (7th Cir. 2022).

Multiplicity is thus a matter of statutory interpretation. *See Elliott*, 937 F.3d 1310, 1313 (10th Cir. 2019). The Court begins with the text of the statute, specifically the “actus reus” of the crime. *Haas*, 37 F.4th at 1261; *Naidoo*, 995 F.3d at 380 (explaining that to assess multiplicity, the court looks “to the statute charged to ascertain the ‘allowable unit of prosecution’ or the *actus reus* of the crime.”). *See also United States v. Elliott*, 937 F.3d 1310, 1313 (10th Cir. 2019) (determining whether multiple counts of 18 U.S.C. § 2252A(a)(5) by reference to the actus reus of the statute). If the text alone is insufficient to ascertain the allowable the unit of prosecution, the Court may consider the legislative history and overall statutory scheme. *United States v. Podell*, 869 F.2d 328, 331 (7th Cir. 1989). If, after that examination, the Court determines the statute is ambiguous, it must “resolve doubts in favor of lenity for the accused.” *Id.*

A. Counts 4, 6, 8, 10 are not multiplicitous.

Defendant has been charged with four counts of violating § 1030(a)(2)(C) of the Computer Fraud and Abuse Act (CFAA). Section 1030(a)(2)(C) criminalizing the act of “access[ing] a computer without authorization . . . and thereby obtain[ing] . . . information from any protected computer.” 18 U.S.C. § 1030(a)(2)(C).

Defendant argues that § 1030(a)(2)(C) is ambiguous as to the unit of prosecution due to its use of the term “any,” and therefore this Court should apply the rule of lenity. In *Bell v. United States*, 349 U.S. 81, 83 (1955), the court considered the allowable unit of prosecution for the Mann Act, 18 U.S.C. § 2421, which made it a crime to “knowingly transport in interstate or foreign commerce *any woman or girl* for the purpose of prostitution or other immoral purpose.” *Bell*, 349 U.S. at 82 (citing 18 U.S.C. § 2421 (1995)). The defendant had, in a single trip, simultaneously transported two women across state lines in the same vehicle, and he was charged with two counts of violating § 2421. *Bell*, 349 U.S. at 82. The court found that the statute was ambiguous as to whether this conduct should qualify as one violation or two, and it held that this “doubt will be resolved against turning a single transaction into multiple offenses.” *Id.* at 84. Therefore, it concluded that the defendant could not be convicted on two separate counts for making a single trip with two women. *Id.* Defendant also cites *Ladner v. United States*, 358 U.S. 169 (1958), where the defendant filed a single shot and injured two federal officers, and the court considered

whether this should give rise to one offense or two under 18 U.S.C. § 254. That statute punished, “Whoever shall forcibly resist, oppose, impede, intimidate, or interfere with any person...while engaged in the performance of his official duties, or shall assault him on account of the performance of his official duties.” 18 U.S.C. § 254 (1940). As in *Bell*, the court held that if “Congress desires to create multiple offenses from a single act affecting more than one federal officer,” it should make that clear, and thus the charged conduct could only result in one count under § 254.

But no such ambiguity exists here. The plain language of § 1030(a)(2)(C) confirms that the “unit of prosecution” is each act of access of a computer without authorization and thereby obtaining of information from a protected computer. A “protected computer” is one that is “used in or affecting interstate or foreign commerce or communication.” 18 U.S.C. § 1030(e)(2). Counts 4, 6, 8, and 10 each allege a separate and distinct instance in which Defendant accessed, without authorization, a protected computer (Twitter’s server(s)) and thereby obtained information; each instance occurred through the hacking and seizing of a separate Twitter account, on a separate date. [161]. Accordingly, the Court need not look beyond the statute’s plain text here to conclude that Counts 4, 6, 8, 10 allege distinct violations, and that they are therefore not multiplicitous. The Court denies Defendant’s motion to dismiss Counts 4, 6, 8, and 10 on multiplicity grounds, [340].

B. Counts 5, 7, 9, and 11 are not multiplicitous.

The Court next considers Defendant’s motion to dismiss Counts 5, 7, 9, and 11 as multiplicitous, which allege violations of the material support statute, 18 U.S.C. § 2339B. Defendant argues that § 2339B does not clearly authorize multiple punishments for individual acts of providing “services” to a foreign terrorist organization, and therefore he may not be convicted of more than one count of providing services to a foreign terrorist organization. [341] at 7.

The Court again begins with the text of § 2339B, which criminalizes the act of “knowingly provid[ing] material support or resources to a foreign terrorist organization, or attempt[ing] or conspir[ing] to do so.” 18 U.S.C. § 2339B (a)(1). Defendant contends the most “natural” reading of this statute is it penalizes a “course of conduct,” not individual acts of support, by reference to dictionary definitions defining support as “the act of process of supporting,” and “resources” as a “source of supply or support.” [341] at 7. But this Court need not resort to dictionaries where Congress itself has provided a clear definition of “material support and resources” in the statutory text:

“material support or resources” means any property, tangible or intangible, or service, including currency or monetary instruments or financial securities, financial services, lodging, training, expert advice or assistance, safehouses, false documentation or identification,

communications equipment, facilities, weapons, lethal substances, explosives, personnel (1 or more individuals who may be or include oneself), and transportation, except medicine or religious materials;

18 U.S.C. § 2339A; *see also* 18 U.S.C. 2239B(g)(4).

Applying this definition, § 2339B criminalizes the act of providing any property or service to a foreign terrorist organization.³ Therefore, each act of providing property or a service to a foreign terrorist organization qualifies as an allowable unit of prosecution, provided there is a meaningful difference in the charged conduct. *See United States v. Khan*, 71 F.3d 367, 376 (7th Cir. 2014) (looking to actus reus of statute for unit of prosecution); *see also Elliott*, 937 F.3d at 1313 (“The ‘unit of prosecution’ is ‘the minimum amount of activity a defendant must undertake, what he must do, to commit each new and independent violation of a criminal statute.’”) (quoting *United States v. Rentz*, 777 F.3d 1105, 1109 (10th Cir. 2015) (en banc)).

Defendant contends, as he did with respect to § 1030(e)(2), that the use of the word “any” renders § 2339B ambiguous as to the unit of prosecution. Defendant relies upon *Elliott*, where the court considered the unit of prosecution for § 2252A(a)(5)(B), which criminalizes the act of “knowingly possess[ing]...any book, magazine, periodical, film, videotape, computer disk, or *any* other material that contains an image of child pornography.” 18 U.S.C. § 2252A(a)(5)(B). There, the defendant, on a single occasion, was alleged to have knowingly possessed multiple electronic devices containing child pornography simultaneously at a single location. *See Elliott*, 937 F.3d at 1312. The court held that the actus reus of the statute was “possession of a storage device.” *Id.* Because the devices were possessed simultaneously, the court applied the rule of lenity, consistent with *Bell* and *Ladner*, to hold that this conduct only constitute one count. *Id.* at 1312–13.

But the challenge present in *Elliott*, *Bell*, and *Ladner*, is not present here. For example, the indictment does not allege that Defendant, on a single occasion, provided more than one “service” to ISIS by distributing two pro-ISIS videos on Twitter, and in turn, charge each video as a separate count. Rather, the indictment alleges several discrete instances of Defendant “providing” a “service” to ISIS by creating and publishing separate content, on several dates, through separate Twitter accounts.⁴

³ Although the statute is clear and the Court need not look further, this interpretation of the unit of prosecution for § 2339B remains consistent with the statute’s stated purpose, which was based upon a finding that foreign terrorist organizations “are so tainted by their criminal conduct that any contribution to such an organization facilitates that conduct.” *See Holder v. Humanitarian Law Project*, 561 U.S. 1, 7 (2010) (citing Antiterrorism and Effective Death Penalty Act of 1996, § 301(a)(7), 110 Stat. 1247, note following 18 U.S.C. § 2339B (Findings and Purpose)).

⁴ The government has specified the following facts it will need to establish to prove Counts Five, Seven, Nine, and Eleven, respectively:

As the Seventh Circuit has acknowledged in other cases, determining when separate postings should qualify as a distinct act of “providing” a “service” to ISIS may be context dependent. *Haas*, 37 F.4th at 1363 (explaining that what specifically qualifies as a “threat” qualifying for a separate count is a “context” and “fact-intensive” inquiry). Here, the indictment draws reasonable lines. *See id.* (finding that the unit of prosecution for 18 U.S.C. § 115 was each individual threat, and that the indictment alleging that the defendant sent three messages containing similar content appropriately charged the messages as separate counts where each contained a complete threat, even where two were only 27 minutes apart); *see also United States v. Khan*, 771 F.3d 367, 376–77 (7th Cir. 2014) (noting that defendants made multiple purchases of contraband cigarettes in violation of statute prohibiting the purchase of contraband cigarettes, over a four-month period, and the distinct purchases qualify as separate transactions under the statute).

Defendant next argues, citing *Universal C.I.T. Credit Corporation*, 344 U.S. 218, 221 (1952), that his acts of providing “services” stem from a “single managerial decision” on his part, namely, the conspiracy charged in Count 1, and therefore he can only be charged as one violation. [341] at 13. In *Universal*, the defendant was charged with 32 violations of the Fair Labor Standards Act for failure to pay wages. *Universal*, 344 U.S. at 219–221. Considering the text and legislative history of the FLSA, the court concluded that the offense made punishable under the FLSA is “a course of conduct, not individual acts.” *Id.* at 224. Accordingly, the court stated, all actions stemming from the same “managerial decision” would qualify as one offense. *Id.* The Court therefore ordered consolidation of the 32 counts into three. *Id.*

-
- “On September 17, 2018, he tweeted from Twitter Account A an ISIS video titled ‘Jihad Goes on Till the End of Time’” (Count Five);
 - “[O]n September 19, 2018, he tweeted from Twitter Account B tweets related to Americans killed in the Anbar dessert” (Count Seven);
 - “[O]n September 25, 2018 he tweeted from Twitter Account C, ‘The body of the brother you see in the video broadcast by A`maq Agency of the Islamic State regarding the attack on the city of al-Ahwaz, southern Iran. Slap the foolish, despicable and corrupt media people who said that the video is fake and there is no proof they are those who carried out the attack’” (Count Nine);
 - “[O]n October 7, 2018, he tweeted from Twitter Account D ‘#Iraq: Destruction of two military vehicles belonging to the Rejectionists army and another belonging to the federal police in addition to the killing and wounding all those who were aboard in #Kirkuk. Praise the Lord – and His Grace!’” (Count Eleven).

[345] at 9–10.

But *Universal* rested on the unique interpretation of the FLSA. As a result, the case has been given limited application,⁵ and provides insufficient support for Defendant's argument here. See *United States v. Makres*, 598 U.S. 1072, 1078 (7th Cir. 1979) (noting in a case charging the defendant with possession of stolen mail on three specified dates, that *Universal* "is based on the legislative history of the statute there involved," and it "provides no support for the argument Makres makes here"). The test for what qualifies as a "separate and distinct act" for multiplicity purposes remains the unit of prosecution authorized by statute. Defendant's proposed test, asking whether the violations were the result of a single "decision" on his part, is not supported by the text and it would lead to the absurd result of enabling defendants to escape additional liability for multiple violations of a criminal statute merely because they decided once to do so.

In short, the text of § 2339B allows for prosecution for each act of providing property or service to a foreign terrorist organization. Counts 5, 7, 9, and 11 each allege separate and distinct instances of Defendant providing a "service" to a foreign terrorist organization, through the posting of separate content, on separate dates, using separate Twitter accounts. The indictment appropriately charged these acts as separate counts. Therefore, the Court denies Defendant's motion to dismiss Counts 5, 7, 9, and 11 as multiplicitous.

C. Government's Santiago Motions [305] [377]

The government has filed a proffer, [305] and a supplemental proffer, [377], seeking to admit co-conspirator statements under Federal Rule of Evidence 801(d)(2)(E) and *United States v. Santiago*, 582 F.2d 1128 (7th Cir. 1978), *overruled on other grounds by Bourjaily v. United States*, 438 U.S. 171 (1978). Rule 801(d)(2)(E) permits the admission of co-conspirator statements as non-hearsay, and *Santiago* permits this Court to conditionally admit the co-conspirator statement "before the conspiracy has been independently established, but subject to the subsequent fulfillment of that critical condition" at trial. *Id.* at 1130–31; *United States v. Davis*, 845 F.3d 282, 286 (7th Cir. 2016); *United States v. Alviar*, 573 F.3d 526, 540 (7th Cir. 2009); *United States v. Harris*, 585 F.3d 394 (7th Cir. 2009). This Court possesses discretion in fashioning a procedure to make this preliminary admissibility determination. *United States v. McClellan*, 165 F.3d 535, 553 (7th Cir. 1999) (citing *United States v. Rodriguez*, 875 F.2d 404, 409–10 (7th Cir. 1992) (discussing methods by which district court can make preliminary determination of admissibility)).

⁵ See *United States v. Billingslea*, 603 F.2d 515, 519 (5th Cir. 1979) ("Because the decision rested on the Court's interpretation of the legislative history of the FLSA, and because *Universal* appears to have been given limited application, we do not feel that it controls the decision in this case."); *United States v. Cohen*, 384 F.2d 699, 700 (2d Cir. 1967) (noting that *Universal* "has received rather limited application beyond the specific situation there presented").

To admit a co-conspirator statement under *Santiago*, the government must show, by a preponderance of the evidence, that: “(1) a conspiracy existed; (2) defendant and the declarant were members of the conspiracy; and (3) the statement was made during the course and in furtherance of the conspiracy.” See *United States v. DeKelaita*, 875 F.3d 855, 859–60 (7th Cir. 2017); see also Fed. R. Evid. 801(d)(2)(E). If the government satisfies this burden, then the statements are not hearsay, and the jury may consider them for any purpose, including their truth. See *United States v. Thompson*, 944 F.2d 1331, 1345 (7th Cir. 1991).

In making this conditional admissibility determination, the Court may consider the proffered statements themselves as evidence of both the existence of a conspiracy and the defendant’s participation in the conspiracy, but the contents of the statements must also be corroborated by at least some supporting evidence. *Harris*, 585 F.3d at 398–99; see *Bourjaily*, 438 U.S. at 180. Such evidence may be either direct or circumstantial. See *United States v. Johnson*, 592 F.3d 749, 754–55 (7th Cir. 2010); see also *United States v. Pust*, 798 F.3d 597, 603 (7th Cir. 2015) (“Circumstantial evidence may be used to establish the existence of a conspiracy and a defendant’s involvement in the conspiracy.”). Here, the government filed a detailed proffer, and supplement, summarizing the nature of the conspiracies charged⁶ and the evidence that the government intends to produce at trial; the proffer includes a representative sample of the co-conspirator statements the government seeks to admit. See, e.g., *McClellan*, 165 F.3d at 553 (holding that government’s *Santiago* proffer need not list out each and every co-conspirator statement to be sufficient). As for the trial evidence, the proffer previews that it will include, among other things, “screenshots” taken by an FBI covert employee of statements made by Khattab members, including Defendant, in two Telegram channels. [305] at 16–17. In those conversations, Khattab members discuss Defendant, and his “head writer” role for Khattab. *Id.* at 17. According to the proffer, the screenshots also include statements by Khattab members “inciting violence,” coordinating Twitter “raids,” and sharing methods to gain unauthorized access to accounts. *Id.* at 18. As one example of a statement regarding violence (among several others provided), the government cites a statement by Defendant stating: “Post it brothers, to cause confusion and spread terror within the hearts of those who disbelieved.” *Id.* at 26. In another example from 2017, a Khattab member describes to the “General Group” action to take during a Twitter raid⁷: “1. Copy the tweet from here 2. Paste it in your personal page on Twitter 3. Keep doing this until your account is DELETED. Easy?” *Id.* at 33.

⁶ The proffer provides a detailed overview of three conspiracies charged in the indictment: the conspiracy to provide material support to a foreign terrorist organization; the conspiracy to provide threats in interstate commerce; and the conspiracy to commit computer fraud. See [305].

⁷ “Twitter raids” reference coordinated instances in which Khattab members hacked into and seized Twitter accounts belonging to third parties for the purposes of posting pro-ISIS content. See [305] at 33–35.

The government indicates in its proffer that it expects these co-conspirator statements will demonstrate, among other things: Khattab members' allegiances to ISIS through examples of members pledging "bayah" (allegiance) to ISIS' leaders; the agreement among Khattab members to promote ISIS' goals of inciting terror and violence against its enemies; Khattab members' efforts to "follow the instructions" of ISIS official media; Khattab's connection to ISIS' official media organizations; and Khattab's responses to instructions from ISIS official groups. *Id.* at 16–18.

Defendant challenges only the first requirement, that the government has established the existence of a conspiracy, *see DeKelaita*, 875 F.3d at 859–60. [393]. A conspiracy exists "when two or more people agree to commit an unlawful act, and the defendant 'knowingly and intentionally' joins in the agreement." *United States v. Bey*, 725 F.3d 643, 648 (7th Cir. 2013) (citing *Johnson*, 592 F.3d at 754).

Defendant argues that he did not agree to commit any unlawful act because all of his actions were lawful, for the same reasons stated in his motion to dismiss, [393] at 3–5. Defendant claims he could not have conspired to violate the material support statute because his actions constituted "independent advocacy," which remains protected under the First Amendment; he could not have conspired to "transmit threats in interstate commerce" because no "true threats" were communicated; and he could not have conspired to violate the CFAA because the government has not properly alleged a CFFA violation. *Id.* As explained below in resolving Defendant's motion to dismiss, the Court rejects those arguments at this stage of the proceedings.

Next, Defendant argues that the government has failed to establish a conspiracy because it has failed to reveal the identity of alleged Co-Conspirators A, B, C, and D, and therefore it remains conceivable that each of these individuals is a government agent or informant. [393] at 5–7. As explained above, however, this Court ordered the government to furnish to Defendant information connecting each co-conspirator designated in the indictment as Co-Conspirator A, B, C, D, to their respective Twitter handles. *See* [396]. At the June 25, 2024 motion hearing, the government represented that, based upon its investigation, none of the conspirators are government personnel, and certainly none are United States government personnel. Should the government fail to prove that a relevant co-conspirator is a non-government agent at trial, the Defendant remains free to make timely objections at trial and this Court will take appropriate remedial action if needed. At this stage, however, the government's proffer undermines the Defendant's request to exclude the statements pretrial on this basis.

Finally, Defendant argues that the government's allegations regarding Mr. Mothafar in its supplemental *Santiago* motion do not establish a conspiracy. [393] at 7–9. Specifically, Defendant states that the government's proffer does not make clear whether Mothafar was a Khattab member, a leader of an adjacent group sharing the same goals, neither, or both. *Id.* at 8. Additionally, Defendant argues that the

government is “tepid” in its motion about whether Mothafar will testify regarding the existence of conspiracy with Defendant, or between any other unidentified members of Khattab. *Id.*

The Court disagrees. First, the Government’s supplemental *Santiago* motion incorporates by reference the government’s initial *Santiago* motion, [305], whose allegations sufficiently establish the existence of a conspiracy. Moreover, the government’s supplemental *Santiago* motion, expressly states that Mothafar served as “the founder of another ISIS supporter media foundation ‘Sunni Shield’ and its related magazine ‘An Anfal.’” [377] at 2. The government details Mothafar’s anticipated testimony, which it proffers will include testimony describing how Mothafar connected with Khattab members, including Defendant, over Telegram and the nature of Mothafar’s communications and relationship with Defendant. *Id.* at 3–5. For example, in one communication, Defendant “defended Khattab’s commitment supporting ISIS” and in another, Mothafar inquired with Defendant about the possibility of purchasing phone numbers to create accounts on Twitter and Facebook, and the use of Virtual Private Networks to hide one’s location during these activities. *Id.* at 4. Taking these allegations together, the proffer suffices; as noted above, the government need not specify every statement to meet its burden under Rule 801(d)(2)(E). *See McClellan*, 165 F.3d at 553.

Although Defendant does not challenge the point, the government has also proffered evidence to show that these statements appear to have been made during and in furtherance of the alleged conspiracies. As a result, the Court conditionally admits these statements, subject to later proof of the *Santiago* factors by a preponderance of evidence at trial.

III. Defendant’s Omnibus Motion to Dismiss the Indictment and Suppress Evidence [372]

A. Defendant’s Motion [372] is Denied as Untimely under Rule 12

Federal Rule of Criminal Procedure 12(b)(3) sets forth a list of motions that must be made before trial, including motions for a “defect in the indictment” and “suppression of evidence.” Fed. R. Crim. P. 12(b)(3)(A). The deadline for filing these motions is set by the Court, or if not set, the deadline becomes the start of trial. Fed. R. Crim. P. 12(c). If not made before the deadline, such a motion is untimely, but a district court may consider the motion “if the party shows good cause.” Fed. R. Crim. P. 12(c)(3). Whether to consider the motion is left to the sound discretion of the district court. *See, e.g., United States v. McMillian*, 786 F.3d 630, 636 n.4 (7th Cir. 2015) (explaining “we ask whether the district court would have abused its discretion had it denied a request to present an untimely motion”).

Defendant's motion is untimely. Defendant filed this motion on April 30, 2024, over 16 months after this Court's set pretrial motion deadline of January 3, 2023. [336].⁸ Even if this Court had not imposed a filing deadline, this Court's standing order also provides, as a default, that all substantive motions must be filed no later than 45 days before the pretrial conference. When the motion was filed, the pretrial conference remained scheduled for May 14, 2024, making the default deadline April 1, 2024. Even applying this later deadline, Defendant filed his motion a month too late.

After missing all pretrial motion deadlines, at the status conference held on April 24, 2022, Defendant proffered that he planned to file two additional, discrete motions: (1) a motion to suppress; and (2) a motion regarding the "status of Twitter." *See* [370]. Based upon Defendant's representation, this Court allowed those "discrete" motions, but it set a deadline of April 29, 2024. *Id.* Here again, counsel failed to meet the deadline, and the motion filed differs dramatically from the motion described in court. Far from the "discrete" motions described, Defendant filed a 72-page motion, raising not only the motion to suppress and Twitter issues, but also three new, undisclosed arguments seeking dismissal of several counts of the indictment on vagueness and First Amendment grounds, along with a motion to quash the search warrant. Had Defendant disclosed the full scope of his proposed untimely motion, the Court would not have permitted any of the untimely motions to be filed. Indeed, this Court has yet to give Defendant leave to file the multiple motions to dismiss raised in [372], aside from that involving Twitter, or the motion to quash. And even if it had, the Defendant again failed to comply with the Court-ordered deadline or otherwise establish good cause for the delay.

Indeed, to date, Defendant still has not alleged "good cause" to file the present motion in an untimely fashion. Nor could he. The Second Superseding Indictment at issue in these motions was filed over four years ago, on March 12, 2020, and Defendant has been represented by counsel since May 11, 2023, over a year before this motion was filed, [356]. Moreover, all of the issues raised in Defendant's untimely motion are based upon facts and law that existed prior to this Court's set deadline of January 3, 2023, and before the Court's standing order deadline of April

⁸ The initial indictment in this case was filed on November 15, 2018. [25]. This Court set the first pretrial motion deadline for November 13, 2020 [191], and extended that deadline through December 11, 2020, [212]. Due to the COVID-19 pandemic, this Court continued the first trial date and provided Defendant a new pretrial motion deadline of March 19, 2021. [237]. Multiple trial dates were set and continued, and deadlines again extended. On April 6, 2022, defense counsel Patrick Boyle was appointed to represent the defendant. [320]. On July 13, 2022, this Court ordered Defendant to file any pretrial motions before September 2, 2022, [325], and further extended that deadline until January 3, 2023. [336]. That was the latest pretrial motion deadline set in this case.

1, 2024.⁹ Further, Defendant claimed during the hearing held on May 8, 2024 that he “could not find” a pretrial motion deadline on the docket and did not read this Court’s standing orders; that systemic lack of diligence undermines any claim of good cause.

For its part, the government has articulated prejudice that would result if the Court were to allow these untimely motions. [389] at 6–7. The statute of limitations for Counts 2, 3, 4, 6, 8, and 10 lapsed in September and October 2023. *Id.* Thus, if these counts were to be dismissed on the merits, the government could not return to the grand jury. *Id.* Although not determinative, the Court considers this argument as part of its analysis.

In sum, 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, 862 (7th Cir. 2007). The government, the Defendant, and the public have an interest in the timely resolution of this case, and thus all parties must honor this Court’s deadlines. The Court therefore denies Defendant’s omnibus motion as untimely and for the lack of good cause. *See United States v. Adkinson*, 609 (7th Cir. 2019) (citing *United States v. Suggs*, 703 Fed. App’x 425, 426 (7th Cir. 2017) (holding district court did not abuse its discretion in declining to consider an untimely motion)).¹⁰

B. Defendant’s Omnibus Motion [372] Fails on the Merits

As explained above, this Court denies Defendant’s omnibus motion to dismiss and suppress [372] as untimely and in violation of this Court’s standing orders and Local Rule 7.1. Even if Defendant’s omnibus motion did not fail for those procedural reasons, however, it nonetheless would also fail on the merits for the reasons explained below, and this Court also denies the motion on that alternative basis.

1. Motion to Quash

Defendant moves to quash the warrant to search his home and various electronic devices located inside, and to suppress any evidence derived from that

⁹ When asked on the record on May 8, 2024 to show good cause to file the untimely motion, counsel for defendant responded, “The good cause is we are not going to be ready for trial, Your Honor.” Obviously, that explanation does not establish good cause.

¹⁰ In addition to being filed late, the Defendant’s filing also violated Local Rule 7.1 and this Court’s standing order incorporating that rule. Local Rule 7.1 provides that briefs in support of any motion shall not exceed 15 pages without prior approval of the court. L.R. 7.1. This Court’s standing orders further direct that the “fifteen (15) page limitation on all memoranda contained in Local Rule 7.1 shall be strictly enforced.” Defendant’s motion was 72 pages, almost five times the permitted length. Again, Defendant did not request leave to file such an extensive brief. The Court denies Defendant’s motion [372] on this additional basis.

search. In a four-corners attack on the affidavit,¹¹ Defendant argues that allegations that he: (1) used a Virtual Private Network; and (2) deleted data from devices before entering the country following a trip abroad remain insufficient to establish probable cause that he was engaged in terrorism. [372] at 41. Defendant further argues that the “crimes” alleged remain “100% protected” by the First Amendment. *Id.* The Court rejects both arguments.

The Fourth Amendment of the U.S. Constitution provides that “no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.” U.S. CONST. amend. IV; *see also United States v. McMillian*, 786 F.3d 630, 638 (7th Cir. 2015). Whether probable cause exists is a “commonsense, practical question” whose answer rests on the totality of the circumstances of the case. *Illinois v. Gates*, 462 U.S. 213, 230 (1983).

Under *Gates*, the relevant circumstances encompass the entire factual record, including rational inferences drawn from the facts based upon the experience of law enforcement. *Id.* In assessing probable cause, the Court “does not deal with hard certainties,” but rather “with probabilities.” *Id.* (quoting *United States v. Cortez*, 449 U.S. 411, 418 (1981)). Although probable cause requires “something more than a hunch,” it does not require a finding that an individual actually engaged in any unlawful activity. *Abbott v. Sangamon Cty., Ill.*, 705 F.3d 706, 714 (7th Cir. 2013). Probable cause requires “only a substantial chance of criminal activity.” *United States v. Schaafsma*, 318 F.3d 718, 722 (7th Cir. 2003). Therefore, probable cause may exist even though there “could have been innocent explanations” for a defendant’s actions, so long as “the inference of the criminal activity was reasonable.” *United States v. Gary*, 790 F.3d 704, 707–708 (7th Cir. 2015) (citing *United States v. Funches*, 327 F.3d 582, 587 (7th Cir. 2003)). Likewise, a prior judge’s probable cause finding enjoys “a strong presumption of correctness,” and will not be disturbed if the judge had “a substantial basis for concluding that probable cause existed.” *United States v. Gibson*, 996 F.3d 451, 461 (7th Cir. 2021) (quoting *United States v. Sanchez-Jara*, 889 F.3d 418, 421 (7th Cir. 2018) and then *Gates*, 462 U.S. at 238–39).¹²

¹¹ The affidavit in support of the search warrant incorporates by reference the more detailed and extensive affidavit filed in support of the complaint and arrest warrant. *See* [389-1]. Collectively, these affidavits will be referenced herein as “the affidavit.”

¹² The “essential protection of the warrant requirement” lies in the requirement that the “usual inferences that reasonable people draw from evidence be drawn by a neutral and detached magistrate.” *United States v. Glover*, 755 F.3d 811, 815-16 (7th Cir. 2014) (internal quotation omitted). As such, the initial judicial “determination of probable cause is given great deference on review, and the Fourth Amendment requires no more than a substantial basis for concluding that a search would uncover evidence of a crime.” *Id.* (citing *Gates*, 462 U.S. at 236). Likewise, the Seventh Circuit reviews “de novo” the “district judge’s decision as to whether a previously issued warrant was supported by probable cause,” but gives “‘great deference’ to the issuing judge’s determination of the existence of probable cause.” *Burnside*, 588 F.3d at 519 (quoting *Gates*, 462 U.S. at 236). *See also*

Applying the *Gates* standard to the factual record here, the Court has little difficulty concluding that probable cause supported the search warrant in this case. The affidavit sets forth details of the investigation relating to Defendant, Khattab, and their pro-ISIS activities on Social Media Applications. *See* [389-1]. It explains that an FBI undercover agent captured numerous conversations between Khattab members, including Defendant, over “Social Media Application,” and cites several examples of those communications. [389-1] at 32–33, ¶¶ 7–8. The conversations reveal tactics Defendant used to conceal his identity and location when engaging in pro-ISIS activities, such as using a separate phone, using a VPN, and communicating in “secret chats.” *See id.* at 10, ¶ 19.¹³

The affidavit also contains specific examples of pro-ISIS infographics and other content Khattab created and posted, including videos “glorifying death in battle on behalf of ISIS” and encouraging others to participate, a video entitled “Our gifts are ready” threatening a terrorist attack, and a video posted by Defendant warning the “Egyptian people” to stay away from polling stations during the March 2018 presidential election. [389-1] at 52–56, ¶¶ 69–77. In addition, the affidavit contains corroborating evidence connecting Defendant and the alleged pro-ISIS activities to the premises and electronic devices searched. *See id.* at 5–20, ¶¶ 11–45. For example, records and physical surveillance from November 2017 through October 2018 confirmed Defendant’s use of multiple phones, including the Subject Phone at an IP address assigned to the Subject Residence. *Id.* at 5–8, ¶¶ 11–17. Those records further reveal that Defendant utilized false subscriber information (name and address) on his iCloud accounts, which law enforcement concluded was another tactic to evade law enforcement. *Id.* at 7–8, ¶ 15.

Furthermore, the affidavit shows that in January 2018, surveillance revealed that Defendant traveled to a region in Iraq, his country of origin, where ISIS had

United States v. Zamudio, 909 F.3d 172, 175 (7th Cir. 2018) (“We review de novo a district court’s determination of probable cause and give great deference to the judgment of the magistrate judge who issued the warrant.”) (citations omitted); *United States v. Scott*, 731 F.3d 659, 665 (7th Cir. 2013) (“a ‘determination of probable cause should be paid great deference by reviewing courts’” and “the duty of a reviewing court is simply to ensure that the judge had a substantial basis for concluding that probable cause existed.”) (quoting *Gates*, 462 U.S. at 236-39) (cleaned up); *United States v. Taylor*, 63 F.4th 637, 652 (7th Cir. 2023) (“We review the district court’s analysis de novo, but we afford great deference to the issuing judge’s finding of probable cause” and “our task is to ensure” that the issuing judge “had a ‘substantial basis for finding the probable cause necessary to support the warrant’”) (quotations omitted).

¹³ For example, on February 19, 2018, the undercover agent (“UCE-1”) asked Defendant if he believes Social Media Application is safe and for his advice regarding security measures. [389-1] at 9. Defendant responded: “Do you have vpn? Have both of them always on and you will be safe by the will of Allah . . . These are all reasonable measures but our security is in Allahs hands. If you are truthful with Allah. He will be at your side. Brother why don’t you make nafir [travel for the purpose of joining jihad]? Do you know about secret chat?” *Id.*

maintained a significant presence. *Id.* at 12–15, ¶¶23–30. When he returned to the United States, Defendant told Customs and Border Protection (“CBP”) in an interview that he uses two applications, WhatsApp and Google Hangouts, neither of which were on his phone; rather, his smartphone was “sanitized” of nearly all applications, media, personal photos, documents, and conversations. *Id.* Based upon the CBP agent’s training and experience, such sanitizing remained typical of “those seeking to avoid detection of their activities including those involved in terrorism” given “the publicly known CBP policy authorizing border searches of electronic devices when entering the country.” *Id.* ¶ 28.

Considering the totality of the circumstances, probable cause existed for the issuance and execution of the search warrant in this case. Accordingly, the Court denies his motion to quash the search warrant for lack of probable cause and denies his motion to suppress evidence recovered in the search conducted pursuant to that warrant.

2. Motion to Suppress

Defendant next moves to suppress evidence the Government obtained via the Stored Communications Act, 18 U.S.C. § 2703(d) (“SCA”). He claims that given the “depth, breadth and comprehensiveness” of the information the government obtained under the SCA, the government needed a warrant supported by probable cause to obtain it. [372] at 45–62. Defendant’s motion to suppress fails on multiple grounds.

As a threshold matter, Defendant has failed, both in his written motion and during oral argument, to sufficiently identify the information he seeks to suppress here. When asked to clarify at the motion hearing, defense counsel generally directed the court to the “list” created and filed by Defendant entitled “Records Obtained via Subpoena/Warrant.” *See* [373], (“Attachment 1”). Attachment 1 purports to list records the government obtained pursuant to the SCA or a search warrant, followed by a series of charts without headings and what appear to be Defendant’s notes. *See id.* For several of the listed records, however, the document fails to delineate whether the record was obtained by subpoena or court order, rather than by search warrant. *Id.* Thus, this attachment fails utterly to develop the record, and it remains unclear which records Defendant seeks to suppress. The party seeking suppression “bears the burden of establishing that he had a reasonable expectation of privacy in what was searched.” *United States v. Tuggle*, 4 F.4th 505, 513 (7th Cir. 2021) (quoting *United State v. Scott*, 731 F.3d 659, 663 (7th Cir. 2013)). Defendant’s failure to specify which records he asks this Court to suppress provides ample basis to deny Defendant’s motion. *See United States v. Butler*, 58 F.4th 364 (7th Cir. 2023) (holding that a party waives perfunctory or undeveloped arguments).

Nonetheless, even if one assumes that the government had obtained, and Defendant had properly challenged, all the records as having been “sought”¹⁴ pursuant to the SCA (rather than by search warrant or other lawful means), his motion to suppress still fails, because it fails to establish that obtaining such information without a warrant would constitute an unlawful search under the Fourth Amendment. Here, Defendant objects generally to: (1) financial information (bank account, credit card numbers, and tax information); (2) non-content text and call information records (phone numbers of senders and recipients); (3) device registration and user activity information, including dates and times of logins for services like Facebook and Twitter (“IP connection information”), and (4) subscriber information (names and addresses). *Id.* at 49. *Id.*¹⁵

The Fourth Amendment protects the people’s right “to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures.” *United States v. Lewis*, 38 F.4th 527, 533–35 (7th Cir. 2022). Generally, if government action qualifies as a “search,” then the government must obtain a warrant supported by probable cause, unless an exception applies. *Id.* Government action may qualify as a search when the government obtains the information or material searched “by physically intruding on a constitutionally protected area,” *United States v. Jones*, 565 U.S. 400, 405 (2012), or when it violates an actual (*i.e.*, subjective) expectation of privacy “that society is prepared to recognize as reasonable.” *Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). In assessing whether a Fourth Amendment search has occurred, the Court draws from “historical understandings ‘of what was deemed an unreasonable search and seizure when the Fourth Amendment was adopted’”, including when deciding whether a “subjective expectation of privacy” was objectively reasonable. *Carpenter v. United States*, 585 U.S. 296, 305 (2018) (quoting *Carroll v. United States*, 267 U.S. 132, 149 (1925)).

To establish a reasonable expectation of privacy in the information obtained pursuant to the SCA, Defendant relies upon *Carpenter*, 585 U.S. at 305. There, the government obtained a court order under the SCA to collect 127 days of historical cell-site location information (“CSLI”)¹⁶ for a robbery suspect’s cell phone number. *Id.*

¹⁴ Defendant’s motion only identifies certain categories of documents that were sought (rather than obtained) pursuant to the SCA. [372] at 48–49.

¹⁵ Defendant also objects to “cell site location data” and “IDs for Apple devices and accounts,” as sought by subpoena, but he also indicates in his motion that CLSI was only obtained in this case with a warrant, and that Apple denied subpoenas for Defendant’s Apple ID information. See [373] at 12 (“Records requested are too broad and could not be provided as it would be too burdensome.”).

¹⁶ Historical CSLI, which was at issue in *Carpenter*, and real-time CSLI, remain distinct, and each requires unique case-specific analysis of the level of intrusion under the fourth amendment. See *United States v. Hammond*, 996 F.3d 374, 383 (7th Cir. 2021). The government’s collection of either type of location information is not at issue here.

at 301–03. The CSLI provided approximately 101 precise location data points each day for the defendant-suspect’s cell phone and showed within 50 meters of accuracy the date and time the cell phone mapped to a location. *Id.* at 303–14. The government used this evidence at trial to secure a conviction, and the defendant appealed. *Id.* at 303.

The Supreme Court held that the government’s level of intrusion in its use of the retrospective historical CSLI records in *Carpenter* constituted a *de facto* tracking device that invaded the defendant’s reasonable expectation of privacy and qualified as a Fourth Amendment search; thus, the government should have obtained a warrant supported by probable cause to obtain such information. *Id.* at 307–316 (citing *Jones*, 565 U.S. at 430 (holding that use of a global-positioning satellite device to track a vehicle’s movements constitutes a search under the Fourth Amendment)). In so holding, the Court emphasized that its decision remained a “narrow one” based upon “novel circumstances” of the case, and thus it did not “call into question conventional surveillance techniques and tools” nor express a view on other matters or investigative tools. *Id.* at 316. Relevant here, the Court also affirmed the validity of “third-party doctrine” despite finding that the doctrine did not justify the type of historical CSLI obtain in *Carpenter*. *Id.* at 308–310, 316; *United States v. Soybel*, 13 F.4th 854, 590 (7th Cir. 2021) (noting that *Carpenter* emphasized that it did not “disturb the application of *Smith* and *Miller*” but merely “declined to extend *Smith* and *Miller* to cover the novel circumstances” presented by historical CSLI in that case).

Even in a post-*Carpenter* world, a defendant normally possesses no reasonable expectation of privacy in information he voluntarily shares with third parties. *See Soybel*, 13 F.4th at 592 (“What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection.”). This principle derives from two cases: *United States v. Miller*, 425 U.S. 435, 443 (1976), where the Court found no reasonable expectation of privacy in banking records which are “voluntarily conveyed to ... banks and exposed to their employees in the ordinary course of business”; and *Smith v. Maryland*, 442 U.S. 735, 740 (1979), where the Court found no reasonable expectation of privacy in telephone records of phone numbers dialed which are “voluntarily conveyed” to the telephone companies. In both cases, the Court held that by voluntarily conveying the information to a third-party company, the defendants had “‘assumed the risk’ that the company’s records ‘would be divulged to the police.’” *Carpenter*, 585 U.S. at 309 (quoting *Smith*, 442 U.S. at 745). Where this “third-party doctrine” applies, the government remains “free to obtain such information from the recipient without triggering Fourth Amendment protections,” such as a search warrant. *Carpenter*, 585 U.S. at 308.

In declining to apply third-party doctrine to the historical CSLI in *Carpenter*, the Court reasoned that, unlike bank transactions and phone calls which require affirmative acts, a cell phone automatically generates CSLI records “without any

affirmative act on the part of the user beyond powering up.” *Id.* at 315. Additionally, the Court reasoned that the nature of CSLI can present considerable and unique privacy concerns because it can provide not only information about a person’s movement or activity “at a particular time,” but it can also retroactively provide a “detailed chronicle of a person’s physical presence compiled every day, every moment, over several years.” *Id.* at 315. Thus, in *Carpenter*, historical CSLI implicated privacy concerns “far beyond” those present in *Miller* or *Smith*. *Id.* at 314 (citing *Miller*, 425 U.S. at 442 and *Smith*, 442 U.S. at 742).

Here, Defendant concedes that historical CSLI is not at issue; the government secured a warrant for the CSLI it obtained. [372] at 56. Defendant instead invites this Court to extend *Carpenter*’s reasoning to other types of records obtained in this case, arguing that given the “vastness and revealing nature” of the information collectively obtained by the government from third parties under the SCA from 2006 through October 17, 2018, the government should have obtained a warrant. *Id.* at 50, 62. The Court declines Defendant’s invitation for two reasons.

First, as the government correctly argues in its response, all of these records remain covered by third-party doctrine, which *Carpenter* left undisturbed. All of these records were voluntarily disclosed to third parties, such that this case “bears the hallmarks of *Smith*, not *Carpenter*.” *See Soybel*, 13 F.4th at 593.

Under *Miller*, *Smith*, and their progeny, Defendant possesses no reasonable expectation of privacy in his financial and tax information or non-content phone records in this case, which he voluntarily disclosed to third party companies. *See Miller* 425 U.S. at 441–42; *Smith*, 442 U.S. at 741–42; *Huon v. Mudge*, 597 F. App’x 868, 875 (7th Cir. 2015) (holding that phone users have no reasonable expectation of privacy in their phone numbers dialed); *see also United States v. Sesay*, 937 F.3d 1146, 1152 (8th Cir. 2019) (applying third-party doctrine to checks and deposit slips retained by a bank, income tax returns provided to an accountant, and electricity-usage statistics tracked by a utility company and thus holding defendant had no reasonable expectation of privacy in these records).

By the same logic, Defendant also lacks a reasonable expectation of privacy in his subscriber information and IP connection information. *See Mudge*, 597 F. App’x at 875 (holding that phone users have no reasonable expectation of privacy in their subscriber information or phone numbers dialed); *United States v. Caira*, 833 F.3d 803, 809 (7th Cir. 2018) (holding that individuals have no reasonable expectation of privacy in their IP connection records); *Soybel*, 13 F.4th at 592 (“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) (noting that “every 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).

As the *Soybel* court explained, unlike the historical CSLI obtained in *Carpenter*, “it’s not the case that a defendant creates internet traffic data “without any affirmative act ... beyond powering up.” 13 F.4th at 594. Rather, an “internet user creates connection data by ‘making the affirmative decision to access a website,’ just as the user of a landline generates a telephone-number record solely by choosing to dial it.” *Id.* at 593 (quoting *United States v. Hood*, 920 F.3d 87, 92 (1st Cir. 2019)). See also *Hood*, 920 F.3d at 92 (explaining that an internet user “generates the IP address data . . . only by making the affirmative decision to access a website or application” while with CSLI, “every time a cell phone receives a call, text message, or email, the cell phone pings CSLI to the nearest cell site tower without the cell phone user lifting a finger”). Here, Defendant “took the affirmative step of downloading” phone and social media applications, including Facebook, Twitter, and others, from which certain information was obtained. Thus, the Court rejects Defendant’s undeveloped argument that all of the information, by virtue of simply being on a cell phone, is “automatically revealed.”

Nor does the information obtained share the unique characteristics of the historical CSLI in *Carpenter*. See *Soybel*, 13 F.4th at 598. As noted above, the *Carpenter* court considered that the CSLI in that case enabled the government to “travel back in time to retrace a person’s whereabouts, subject only to the retention policies of the wireless carriers.” *Carpenter*, 585 U.S. at 312. The type of records cited here present no such capabilities and thus do not involve the same level of intrusion. See, e.g., *id.* (explaining that telephone logs “reveal little in the way of identifying information”); *Hood*, 920 F.3d at 90 (explaining that IP-address data, unlike CSLI “is merely a string of numbers associated with a device that had, at one time, accessed a wireless network”). Without explanation, Defendant simply contends that the records cited above somehow “disclose extraordinarily intimate and revealing details” about his personal life, including the workings of his “mind.” [372] at 55. Not so. Indeed, the information here, clearly falling within the third-party doctrine, resembles the telephone pen registers approved in *Smith*. See *Soybel*, 13 F.4th at 598 (rejecting defendant’s argument that information provided a “glimpse into his *mind*,” and an “intimate window” into his relationships) (emphasis in original). In short, the information divulged by each of the records referenced above—records which the government may or may not have accessed without a warrant (it remains unclear)—pales in comparison to the type of “perfect surveillance” the historical CSLI revealed in *Carpenter*. Thus, the unique privacy interests present in *Carpenter* remain absent here.

Unsurprisingly then, the gravamen of Defendant’s argument is not that he possesses a reasonable expectation of privacy under *Carpenter* in certain types of records he claims the government may have obtained without a warrant in this case. Instead, Defendant focuses upon the *volume* of information obtained over a twelve-year investigatory period, which he claims collectively paints the government a

“mosaic” of Defendant’s “private, personal” affairs, such that a warrant was required. But there is no “volume exception” to the SCA, and *Carpenter* did not create one. That information lawfully collected pursuant to the SCA or other statute becomes “extremely voluminous” on its own does not generate a constitutional concern or a new, previously-absent warrant requirement. Likewise, as this Court noted during the motion hearing, that a lawful, investigative technique reveals “intimate or private” information, on its own, does not transform the technique into a Fourth Amendment violation.

In sum, *Carpenter*’s scope remains “narrow.” *Carpenter*, 585 U.S. at 316. The decision left undisturbed third-party doctrine, and in turn, the government’s ability to obtain certain information covered by that doctrine via a court order or subpoena upon a proper showing. This Court declines to create a “volume” exception to the SCA or extend *Carpenter* to require the government to obtain a warrant when it lawfully obtains some ill-defined threshold amount of information that a defendant deems to be “too much.”

In reaching this conclusion this Court does not “discount the importance of the internet” in today’s world. *See Soybel*, 13 F.4th at 593. But in assessing Fourth Amendment challenges, the Court must make a “fact-specific inquiry” to determine whether a defendant has a reasonable expectation of privacy in the subject of the search at hand. *Burnside*, 588 F.3d at 517. As the party seeking suppression here, Defendant bears the burden of establishing he had a reasonable expectation of privacy in the information at issue. *See Tuggle*, 4 F.4th at 513. He has not met that burden. As a result, this Court denies his motion to suppress evidence.

Alternatively, Defendant argues that this Court should suppress evidence obtained in this case (exactly what evidence is again left unidentified) pursuant to the SCA either because: (1) terms of service agreements are not enforceable contracts and thus evidence obtained from third-party providers under the SCA should be suppressed; or because (2) terms of service agreements create a sort of *involuntary bailment*, and therefore “the data is essentially stolen property,” and the government may not use it at trial. [372] at 62–69. For these propositions, Defendant directs the Court only to Justice Gorsuch’s dissent in *Carpenter*, in which the Justice discussed principles of property law and whether they might justify the protection of data belonging to third parties under the Fourth Amendment. *Carpenter*, 585 U.S. at 386–306 (Gorsuch, J., dissenting). In his dissent, Justice Gorsuch noted that “complete or exclusive control of property” is not always a condition to the assertion of a Fourth Amendment right, and thus perhaps the way in which “we store data with third parties” under “functionally compelled” circumstances may amount to a sort of involuntary bailment.” 585 U.S. at 402 (Gorsuch, J., dissenting). Even if such language were to bind this Court—and it does not—it would not support, let alone justify, Defendant’s proposals here. The Court rejects both arguments, which it finds

unsupported and unpersuasive, and thus denies Defendant's motion to suppress for this additional reason.

Finally, even if this Court were to extend *Carpenter* and require a warrant to obtain the information acquired in this case under the SCA, suppression would still not be the appropriate remedy. When law enforcement agents act with an "objectively reasonable, good-faith belief that their conduct is lawful," the exclusionary rule does not apply. *Hammond*, F.3d at 392. Here, the information obtained pursuant to the SCA was not the type of historical CSLI requiring a warrant under *Carpenter*. Rather, as the government indicates in its Response, this information falls squarely within third-party doctrine. As such, suppression would not be the appropriate remedy. The Court thus denies Defendant's motion to suppress on this independent basis as well.

3. Motion to Dismiss Counts 1, 5, 7, and 9

Defendant next seeks to dismiss Counts 1, 5, 7, and 9 of the indictment, which charge him with conspiracy to violate, and substantively violating, the material support statute, 18 U.S.C. § 2339B(a)(1). Section 2339B criminalizes "knowingly providing material support or resources to a foreign terrorist organization." 18 U.S.C. § 2339B(a)(1). The statute defines "material support or resources" as "any property, tangible or intangible, or service," *See* § 2339A(b)(1); *see also id.* § 2339B(g)(4).

Defendant argues that § 2339B is unconstitutionally vague and overbroad. [372] at 5. He further argues that his actions underlying these counts constitute protected First Amendment activity, and that his actions were not done "in coordination with or at the direction of" a foreign terrorist organization. [372] at 5. The Court addresses these arguments in turn.

a. The material support statute is neither unconstitutionally vague nor overbroad.

Void-for-vagueness doctrine is an outgrowth of the Due Process Clause of the Fifth Amendment, while overbreadth doctrine is an outgrowth of the First Amendment. *See United States v. Williams*, 553 U.S. 285, 304 (2008).¹⁷ Although

¹⁷ In the First Amendment context, although vagueness and overbreadth remain distinct doctrines, they are "often conceived as 'alternative and overlapping' theories for relief on the same type of claim." *Ctr. for Individual Freedom v. Madigan*, 697 F.3d 464, 479 (7th Cir. 2012); *see also Entertainment Productions, Inc. v. Shelby Cnty.*, 588 F.3d 372, 379 (6th Cir.2009) ("When a law implicates First Amendment freedoms, vagueness poses the same risk as overbreadth, as vague laws may chill citizens from exercising their protected rights."); Richard H. Fallon, Jr., *Making Sense of Overbreadth*, 100 Yale L.J. 853, 904 (1991) ("First Amendment vagueness doctrine—as distinct from ordinary or non-First Amendment vagueness doctrine—is best conceptualized as a subpart of First Amendment overbreadth doctrine.").

these doctrines are distinct, each is based upon the “fundamental principle in our legal system” that laws which “regulate persons or entities must give fair notice of conduct that is forbidden or required.” *F.C.C. v. Fox Television Stations, Inc.*, 567 U.S. 239, 253 (2012). A statute that is overbroad or vague is unconstitutional and invalid. See, e.g., *United States v. Cook*, 970 F.3d 866, 879 (7th Cir. 2020); *United States v. Hansen*, 599 U.S. 762, 769–70 (2023) (discussing overbreadth doctrine).

A statute is unconstitutionally overbroad¹⁸ if it prohibits a substantial amount of speech that is protected under the First Amendment, “not only in the absolute sense, but also relative to the statute’s plainly legitimate sweep.” *Ctr. for Individual Freedom v. Madigan*, 697 F.3d 464, 476 (7th Cir. 2012) (citing *Williams*, 553 U.S. at 292). A statute is unconstitutionally vague if it fails to “define an offense with sufficient clarity that an ordinary person has fair notice of what conduct is prohibited so as to avoid arbitrary and discriminatory enforcement.” *Cook*, 970 F.3d at 872–73 (first citing *Skilling v. United States*, 561 U.S. 358, 402–03 (2010), then citing *United States v. Sylla*, 790 F.3d 772, 774–75 (7th Cir. 2015)).

Where a statute implicates First Amendment freedoms, a “heightened standard” of scrutiny applies. *Madigan*, 697 F.3d at 479. For the sake of resolving Defendant’s motion, the Court assumes without deciding that this is the proper standard to be applied here. See *United States v. Osadzinski*, 97 F.4th 484 (7th Cir. 2024)) (assuming without deciding that defendant’s offense consisted entirely of expressive activity within the meaning of the First Amendment). Nonetheless, even in the First Amendment context, one who engages in clearly proscribed conduct cannot “complain of the vagueness of the law as applied to the conduct of others” in a facial challenge. *Williams*, 553 U.S. at 304. This Court thus considers Defendant’s vagueness claim as applied to the particular facts at issue first. *Holder v. Humanitarian Law Project (“HLP”)*, 561 U.S. 1, 18–19 (2010).

Defendant argues that § 2339B remains impermissibly vague because “a person of ordinary intelligence” would not understand posting political messages on social media platforms to constitute “service” (or “personnel”) within the meaning of the material support statute. [372] at 9. In support, he cites *Humanitarian Law Project (“HLP”)*, which the parties agree is instructive here. In *HLP*, the plaintiffs sought to provide support for two designated foreign terrorist organizations, in the form of monetary contributions, other tangible aid, legal training, and political advocacy. 561 U.S. at 10. They brought a pre-enforcement challenge to § 2339B, alleging that the material support statute’s terms, “training” “expert advice or

¹⁸ Defendant characterizes his overbreadth challenge as an “as-applied” challenge, but all overbreadth challenges are facial challenges in one sense, because an overbreadth challenge by its nature assumes that the measure is constitutional as applied to the party before the court. *In re New York City Policing During Summer 2020 Demonstrations*, 548 F. Supp. 3d 383, 415 (S.D.N.Y. 2021). Thus, the Court construes Defendant’s argument both as a facial one and as applied to this case.

assistance,” “service,” and “personnel,” were unconstitutionally vague, and that the statute violated their First Amendment rights to freedom of speech and association. *Id.* at 11. Specifically, the plaintiffs argued that it remained unclear whether “political advocacy” on behalf of designated terrorist organizations amounted to “material support” in the form of providing “personnel” or “services,” rendering the statute impermissibly vague. *Id.* at 15.

The Supreme Court rejected the argument, explaining that the statute defines “personnel” constituting material support as “knowingly providing a person ‘to work under that terrorist organization’s direction or control or to organize, manage, supervise, or otherwise direct the operation of that organization.’” *Id.* at 23 (citing § 2339B(h)). Indeed, the Court explained, § 2339B “makes clear that ‘personnel’ does not cover *independent* advocacy,” by specifying that “individuals who act entirely independently of the foreign terrorist organization to advance its goals or objectives shall not be considered to be working under the foreign terrorist organization’s direction and control.” *Id.* (quoting § 2339B(h)) (emphasis in original).

Nor was the statute impermissibly vague as to the meaning of “services”; the Court explained:

“service” similarly refers to concerted activity, not independent advocacy. *See Webster’s Third New International Dictionary* 2075 (1993) (defining “service” to mean “the 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”). Context confirms that ordinary meaning here. The statute prohibits providing a service “to a foreign terrorist organization.” § 2339B(a)(1) (emphasis added). The use of the word “to” indicates a connection between the service and the foreign group. We think a person of ordinary intelligence would understand that independently advocating for a cause is different from providing a service to a group that is advocating for that cause.

HLP, 561 U.S. at 23–24.

Therefore, the Court 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.

The indictment alleges that Defendant and his co-conspirators knowingly provided and attempted to provide material support, through the creation and dissemination of pro-ISIS content, “to” ISIS, knowing that ISIS was a designated terrorist organization engaged in terrorist activity. *See* [161]. As the *HLP* Court made clear, the mere fact that speech or conduct—in the abstract—may be protected under the First Amendment remains irrelevant. The allegations that Defendant

engaged in such conduct as a service “to ISIS” transforms protected “independent advocacy” into criminal activity under § 2339B.

United States v. Osadzinski also remains instructive. 97 F.4th 484 (7th Cir. 2024). In that case, the government indicted Osadzinski, like Safoo, under § 2339B, charging him with creating or modifying code, establishing channels in which to use the code, and distributing the code to others for the purpose of preserving ISIS videos and avoid law enforcement detection and interference. *Id.* at 488. Like the defendant here, Osadzinski moved to dismiss the indictment, arguing that the statute was unconstitutionally vague for failing to provide fair notice that “downloading pro-ISIS media for personal viewing and for potentially sharing with others online” might qualify as a “service to a terrorist organization under § 2339B.” *Id.* But the district court rejected the argument, finding that the statute clearly defined that developing propaganda-duplicating computer code in coordination with and at the direction of ISIS constituted criminal conduct. *Id.* at 490. On appeal, the Seventh Circuit agreed, finding that Osadzinski “attempted to engage in activity coordinated with or directed by a known foreign terrorist organization” and that activity was “both unprotected by the First Amendment and clearly violative of § 2339B.” *Id.* at 495.

Here, Defendant further argues that the statute fails to define what level of “direction or control” constitutes providing a “service to a foreign terrorist organization,” making it unconstitutionally vague in this aspect as well. But, as *HLP* explains, “services” within the meaning of § 2339B means “concerted activity” between the defendant and the foreign terrorist organization. *Id.* at 23–24. The government has charged—and must prove at trial—that Defendant acted “in coordination with or at the direction of” ISIS; Defendant’s “Go Cubs Go” example¹⁹ remains untethered to the allegations.

In sum, the material-support statute “provides a person of ordinary intelligence fair notice of what is prohibited.” *Williams*, 553 U.S. at 304, and thus Defendant’s vagueness challenge fails.

Turning to Defendant’s overbreadth challenge, the Court’s “first task is to determine whether the enactment reaches a substantial amount of constitutionally protected conduct [or speech], as judged against the statute’s legitimate sweep.” *Vill. of Hoffman Ests. v. Flipside, Hoffman Ests., Inc.*, 455 U.S. 489, 494 (1982). In making this determination, the statute’s “unconstitutional applications must be realistic, not fanciful, and their number must be substantially disproportionate to the statute’s

¹⁹ Defendant argues that his actions are analogous to a baseball fan holding up a sign that reads, “Go Cubs Go” and asserts that no one would reasonably interpret such action to constituting a “service” to the Cubs. Following Defendant’s analogy, however, the allegations here are not that Defendant did the equivalent of holding up a pro-ISIS sign, but rather that he held up a pro-ISIS sign at the direction of or in coordination with, ISIS. That fact, as noted above, is what transforms his alleged conduct from independent advocacy to criminal activity.

plainly legitimate sweep.” *Hanson*, 599 U.S. at 770 (citing *New York State Club Assn., Inc. v. City of New York*, 487 U.S. 1, 14 (1988)). If the unconstitutional applications do not substantially outweigh the constitutional applications, the overbreadth challenge fails. *Hanson*, 599 U.S. at 770; *Hoffman Estates*, 455 U.S. at 494.

Applying these principles, § 2339B passes constitutional muster. As noted above, § 2339B covers “knowingly” providing “material support or resources to a foreign terrorist organization.” 18 U.S.C. § 2339B(a)(1). Section 2339B also states, however, what it does not cover, through a constitutional savings clause, which provides: “Nothing in this section shall be construed or applied so as to abridge the exercise of rights guaranteed under the First Amendment to the Constitution.” *Id.* § 2339B(i). In considering the First Amendment challenge in *HLP*, the Court relied upon this clause, and it concluded that § 2339 prohibits “only a narrow category of speech” that falls outside the protection of the First Amendment—speech “to, under the direction of, or in coordination with foreign groups that the speaker knows to be terrorist organizations.” 561 U.S. at 26. The statute does “not prevent a person from freely speaking about, or even independently advocating for, a terrorist organization.” *Id.* at 24; *see also Osadzinski*, 97 F.4th at 493 (§ 2339B “does not prohibit persons from expressing sympathy for the views of a foreign terrorist organization”) (citing *Boim v. Quranic Literary Inst. and Holy Land Found. For Relief and Dev.*, 291 F.3d 1000, 1026 (7th Cir. 2022)). Thus, § 2339B does not reach a “substantially disproportionate” amount of protected speech,” *see Hoffman Estates*, 455 U.S. at 494, but rather only a narrow carved-out category of speech done “in coordination with or at the direction of” FTOs.

In making his overbreadth claim here, Defendant poses a hypothetical scenario in which he might be prosecuted under § 2339B for reading pro-ISIS essays aloud as a sermon at his local mosque, rather than for posting them on Twitter. [372] at 11. According to Defendant, “one can imagine the chilling effect such an application of the material support statute would have,” because it would chill both “quintessential political speech” and “religious expression.” *Id.* Defendant’s argument, however, misses the point. Using Defendant’s example, Defendant could not, consistent with *HLP*, be prosecuted under § 2339B for merely delivering a sermon expressing pro-ISIS beliefs. That would amount to independent advocacy, which remains protected under the First Amendment. The distinguishing factor, instead, is whether the reading outside the mosque, Twitter post, or any other pro-ISIS advocacy activity was done “in coordination with or at the direction of” ISIS. Those are precisely the government’s allegations in this case, and thus Defendant’s hypotheticals do not materialize here.

Here, on its face or as-applied, Defendant has failed to show how protected speech may be restrained unconstitutionally under 2339B, and likewise he cites no authority finding § 2339B overbroad. The material-support statute is not overbroad, and the Court denies Defendant’s motion on this basis.

b. Whether Defendant's Actions Satisfy the Elements of the Material Support Statute is a Matter for Trial

Defendant argues that, even if the material-support statute is not vague or overbroad, his posting of political essays and cartoons on Twitter constitutes protected speech under the First Amendment. Relatedly, he argues that “he did not work ‘in coordination with or at the direction of’ ISIS.” [372] at 14. Instead, Defendant claims that his actions amounted to “independent advocacy,” and therefore under *HLP*, such activity is exempt from prosecution under § 2339B.

Again, even though “independent advocacy” remains protected under the First Amendment, posting pro-ISIS political essays and cartoons becomes criminal when it is done “in coordination with, or at the direction of” a foreign terrorist organization, here, ISIS. *See HLP*, 561 U.S. 1. Obviously, it is for this reason that the *Osadzinski* court rejected the defendant’s First Amendment challenge to his conviction. 97 F.4th at 494. The court explained that while *Osadzinski*’s conduct entailed “expressive activity,” the jury found that he “coordinated his actions—or, at the very least, attempted to coordinate them—with ISIS members.” *Id.* at 492. As a result, the court concluded, his actions fell outside of the First Amendment’s protections. *Id.* Should the government fail to prove at trial that Defendant’s alleged creation and posting of political essays, cartoons, and other pro-ISIS expressions, were “in coordination with or at the direction of” ISIS, then he may move for acquittal; for now, the indictment (which alleges that Defendant so acted) precludes dismissal on this basis, and the Court thus denies the motion as to Counts 1, 5, 7, and 9.

IV. Defendant's Motion to Dismiss Count 2

Count 2 of the indictment charges Defendant with conspiring “to knowingly and willfully transmit in interstate commerce communications containing threats to injure the person of another” in violation of 18 U.S.C. § 875(c) and 18 U.S.C. § 371. Defendant argues that this Court should dismiss Count 2 because: (1) the conspiracy statute, 18 U.S.C. § 371,²⁰ is impermissibly vague as applied to him; (2) the interstate threat statute, 18 U.S.C. § 875 is impermissibly vague as applied to him; and (3) no “true threats” were communicated. The Court addresses these arguments in turn.

Recall that a statute is impermissibly vague and violates due process only if it “fails to provide a person of ordinary intelligence fair notice” of what is prohibited, or it is so “standardless that it authorizes or encourages seriously discriminatory enforcement.” *Williams*, 553 U.S. at 304. Thus, in determining whether a statute is vague, the focus is on statutory clarity: if a reasonable person would have been on

²⁰ Defendant’s brief cites 8 U.S.C. § 871, [372] at 19, but this Court construes Defendant’s arguments as referring to 18 U.S.C. § 371, the conspiracy statute.

notice that his or her conduct was at risk, and reasonable guidelines for enforcement exist, then a statute is not unconstitutionally vague. *United States v. Pitt-Des Moines, Inc.*, 168 F.3d 976, 987 (7th Cir.1999); *see also Grayned v. City of Rockford*, 408 U.S. 278, 282 (1972) (“An enactment is void for vagueness if its prohibitions are not clearly defined.”). In assessing vagueness challenges to statutes not implicating First Amendment concerns, courts consider whether a statute is vague “in light of the facts of the particular case—*i.e.*, as applied—rather than in the abstract.” *Cook*, 970 F.3d at 873.

Defendant argues that the conspiracy statute, § 371, is impermissibly vague as applied to him because it does not provide notice of “what level of intent is required” to be held liable of conspiracy to violate the interstate threat statute, and it does not properly define whether a defendant can be held liable if he did not personally author or send the threatening message. *Id.* at 19. Well-established law, however, undermines Defendant’s theory.

To prove a violation of § 371, the government must establish: (1) that the charged conspiracy existed; (2) that the defendant knowingly became a member of the conspiracy with an intent to advance the conspiracy; and (3) that one of the conspirators (not necessarily the defendant) committed an overt act in an effort to advance the goals of the conspiracy. *See United States v. Sorensen*, 684 F.Supp.3d 784, 795 (N.D. Ill. July 31, 2023). Thus, the government must show the defendant acted knowingly but it need not establish that the defendant personally committed the overt acts outlined in the indictment. *See* [161] ¶ 8. The requirements are clear and § 371 is not vague as applied to Defendant’s alleged conduct.

Nor is § 875(c) impermissibly vague as applied to Defendant. According to Defendant, § 875(c) is vague because it does not specify whether a threat must be directed at a “specific person or group” to invoke criminal liability. [372] at 20–21. The statute reads, in relevant part:

Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both.

18 U.S.C. § 875(c).

In *United States v. Khan*, the grand jury indicted the defendant for communicating a threat in violation of 18 U.S.C. § 875(c), specifically for making threatening remarks on his Facebook page. Case No., 18-2612, 2017 WL 3262572, at *4 (N.D. Ill. May 31, 2017), *aff’d*, 937 F.3d 1042 (7th Cir. 2019). The defendant argued that § 875(c) was unconstitutionally vague because an individual “cannot know with any certainty which statements are acceptable and which he is supposed to avoid.”

2017 WL 2362572, at *19. This Court rejected Khan’s vagueness challenge, explaining that “an ordinary citizen can understand what is meant by the terms ‘threat to kidnap’ and ‘threat to injure,’” and thus the statute provides sufficient standards to allow enforcement in a non-arbitrary manner. *Id.* at 20 (quoting *United States v. Sutcliffe*, 505 F.3d 944, 953–54 (9th Cir. 2007)).

On appeal, the Seventh Circuit affirmed the denial of Defendant’s motion to dismiss where the alleged targets threatened by Khan were “college student[s],” “vulnerable individuals,” people “walking their dogs,” “high net worth individual[s],” and “witnesses” that “get [in] the way.” *Id.* at 1046. Here, the indictment describes threat recipients as specific as those in *Khan*: Christians,²¹ citizens of the “United States, the United Kingdom, France, Australia, Russia, and Iraq,” citizens of “Berlin, Brussels, London, Moscow, New York, and Sydney,” “Cross worshippers,” and other “disbelievers.” *See* [161]. As such, the allegations remain sufficient.

In a similar vein, Defendant argues that this Court should dismiss Count 2 because the indictment does not allege a specific person received or viewed the threatening messages. [372] at 23–24. He further asserts that the identified threats do not qualify as “true threats.” *Id.* The “video is so bad,” he says, “anyone who saw it would assume it was made by an elementary child as a crude joke.” *Id.* At this point in the proceedings, the allegations undermine this claim. Here, the indictment identifies the dates and means for how each of the named “threats” was transmitted or communicated, whether on Social Media Application A or over the Internet. Likewise, whether any of the identified “targets” actually viewed the video is not an element of the offense required to be alleged in the indictment, either explicitly or in context. As for whether the threats are “good enough” to qualify as “true threats,” that factual determination remains a question for trial. The Court thus denies Defendant’s motion to dismiss Count 2.

V. Defendant’s Motion to Dismiss Counts 3, 4, 6, 8, and 10

Counts 3, 4, 6, 8, and 10 charge Defendant with conspiring to (Count 3), and intentionally gaining access to a protected computer through Twitter accounts A, B, C, and D and intentionally gained unauthorized access to those computers in violation of the CFAA, 18 U.S.C. § 1030(a)(2) (Counts 4, 6, 8, 10). [161]. The CFAA provides that whoever “intentionally accesses a computer without authorization or

²¹ The indictment, reasonably interpreted, alleges that Christians were the target of the threats. For example, the indictment cites the “Our gifts are ready” video Khattab created and distributed on December 26, 2017, which depicts a “present under a Christmas tree that contains a bomb” with families around it before a soldier detonates the bomb and engulfs the image in flames. Likewise, in December 2017, the indictment alleges that Khattab created and distributed an infographic of a “headless Santa Clause.” *See* [161].

exceeds authorized access,” and thereby obtains “information from any protected computer” shall be punished under the section. 18 U.S.C. § 1030(a)(2).

Defendant argues the indictment fails to sufficiently allege the elements of § 1030(a)(2) because a “Twitter account” is not a protected computer under the CFAA, and accessing a Twitter account does not enable one to “obtain information,” at least “apart from what is accessible to millions of Twitter users.” [372] at 23–26. Alternatively, he argues that the terms “computer” and “unauthorized access” are unconstitutionally vague as applied to him. *Id.* at 27–33. He also contends that the indictment should be dismissed because no “unauthorized access” occurred. *Id.* The Court addresses these arguments in turn.

To be sufficient, an indictment must: “(1) state the elements of the offense charged; (2) fairly inform the defendant of the nature of the charge so that he may prepare a defense; and (3) enable the defendant to plead an acquittal or conviction as a bar against future prosecutions for the same offense.” *United States v. Khan*, 937 F.3d 1042, 1049 (7th Cir. 2019). In making this determination, the “key question” is whether the indictment sufficiently apprised Defendant of the charges against him to enable adequate trial preparation. *Id.* (citing *Vaughn*, 722 F.3d at 927).

Here, the indictment amply satisfies these requirements. As discussed above with respect to Defendant’s motion for a bill of particulars, the indictment alleges that Defendant conspired to “intentionally access a protected computer” *through* Twitter accounts A, B, C, and D. The indictment states that Khattab members were aware that social media accounts were frequently suspended or closed by Twitter, and as a result, the members shared information regarding how to “hack” into and “seize” social media accounts. To seize the accounts, Khattab members created Hotmail email accounts to reset Twitter Account passwords registered to third parties. See [161] at 12, ¶ 6. Once Khattab members reset passwords to access and take over accounts that did not belong to them, they used the accounts to disseminate pro-ISIS information. *Id.* ¶ 5. Moreover, “between August 2018 and October 2018, defendant saved information to his iPhone” from Twitter accounts that he accessed or attempted to access without authorization. *Id.* at 13, ¶ 8(e). These allegations provide fair notice of the alleged CFAA violations. *Vaughn*, 722 F.3d at 927.

Defendant also argues that the indictment fails to state a CFAA violation because a Twitter account is not a “protected computer” within the meaning of the statute. [372] at 23–26. But the government does not contend that the Twitter accounts themselves constitute the protected computers unlawfully accessed here. [382] at 23. More precisely, the indictment alleges that Defendant accessed protected computers *through* Twitter accounts A, B, C, and D, which the government has clarified references Twitter’s servers. In other words, “by accessing these social media accounts, he accessed Twitter’s servers.” *Id.* Moreover, the CFAA explicitly defines “computer” as “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. § 1030(e)(1). A “protected computer” is one that is “used in or affecting interstate or foreign commerce or communication,” *id.* § 1030(e)(2), which practically speaking, means “any computer connected to the internet.” *hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1194–95 (9th Cir. 2022).

Clearly, the CFAA’s specific definitions, as applied to the alleged conduct of Defendant, provide “a person of ordinary intelligence fair notice of what is prohibited,” such that section 1030(a)(2) is not unconstitutionally vague. *Williams*, 553 U.S. at 304. As alleged, the servers fall within the plain language of the CFAA. A “server” is a “data processing device.” *See* 18 U.S.C. § 1030(e)(1). The purpose of a server is to process and retain data. *ACW Flex Pack LLC v. Wrobel*, No. 22-CV-6858, 2023 WL 4762596, at *7 (N.D. Ill. July 26, 2023). Additionally, by their nature, servers operate “in conjunction with” a computer” (quoting 18 U.S.C. § 1030(e)(1)) because they “manage network resources and provide data to other computers.” *hiQ Labs, Inc.*, 31 F.4th at 1195. For these reasons, the Ninth and Eleventh Circuit have squarely held that servers constitute “computers” within the meaning of the CFAA. Servers thus “clearly qualify” “as computers” under the CFAA. *SkyHop Techs., Inc. v. Narra*, 58 F.4th 1211, 1227 (11th Cir. 2023) (quoting *hiQ Labs*, 31 F.4th at 1195). This Court follows suit.²²

Defendant also argues that the indictment fails to allege that Defendant “obtained information” from a protected computer. [372] at 24–26. Not so. Here, the indictment alleges that from the Twitter accounts Defendant accessed without authorization, he “saved information to his iPhone.” [161] at 13, ¶ 8(e). Additionally, even if Defendant had not downloaded or saved any information, the courts have interpreted “obtain information” broadly, as including “mere observation of data.” *See Good 'Nuff Garage, LLC v. McCulley*, No. 3:21CV571, 2022 WL 4485810, at *12 (E.D. Va. Sept. 26, 2022); S. Rep. No. 104-357, at *7, 1996 WL 492169 (1996)

²² Even if the government had only proceeded on the theory that Defendant had unlawfully accessed Twitter accounts, the Court still would not dismiss these counts for failure to state a CFAA violation. Applying the plain language of the CFAA, “most courts hold that unauthorized access to web-based accounts can form the basis of a CFAA violation.” *Hill v. Lynn*, No. 17-cv-6318, 2018 WL 2933636, at *3 (N.D. Ill. June 12, 2018) (collecting cases); *see also Estes Forwarding Worldwide LLC v. Cuellar*, 239 F. Supp. 3d 918, 921, 926–27 (E.D. Va. 2017) (holding plaintiff sufficiently pled access to a “protected computer” when it alleged that defendant accessed a confidential Google Drive); *Brown Jordan Int’l, Inc. v. Carmicle*, 2016 WL 815827, at *3, *40-41 (S.D. Fla. Mar. 2, 2016) (holding defendant could be liable under CFAA when he accessed fellow employees’ email accounts through a web portal from his personal iPad); *Hedgeye Risk Mgmt., LLC v. Heldman*, 271 F.Supp.3d 181, 192 (D.D.C. 2017) (holding plaintiff pled access to a “protected computer” by alleging that defendant accessed electronically stored emails and documents via computer connected to the internet).

(discussing 18 U.S.C. § 1030(a)(2) and stating that because “the premise of this subsection is privacy protection, the [Senate Judiciary] Committee wishes to make clear that ‘obtaining information’ in this context includes mere observation of the data”); *United States v. Drew*, 259 F.R.D. 449, 457 (C.D. Cal. 2009) (holding mere observation of data can constitute obtaining information for CFAA purposes). Thus, Defendant’s argument that he could not “obtain information” by accessing a Twitter account is unavailing.

In sum, the indictment alleges that Defendant and Khattab members intentionally accessed protected computers, by hacking into and seizing Twitter accounts A, B, C, and D, and then used those accounts to disseminate pro-ISIS information. This remains sufficient to put Defendant on notice of the CFAA charges against him. Whether the government’s proof at trial will be sufficient is a different question. *United States v. Lee*, No. 12-cr-109, 2017 WL 56630, at *1 (N.D. Ill. Jan. 5, 2017) (noting “while an indictment may be dismissed if subject to a defense that raises only a question of law, a defense relating to the strength of the government’s evidence ordinarily must wait for trial.”).

Defendant next argues that “unauthorized access” as used in the CFAA is unconstitutionally vague as applied to him. [372] at 31–33. Again, in assessing vagueness, the Court turns to the text of the CFAA. The CFAA does not define “authorization.” See 18 U.S.C. § 1030. As a result, this Court turns to the “fundamental canon of statutory construction” that, unless otherwise defined, words will be “interpreted as taking their ordinary, contemporary, common meaning.” *Perrin v. United States*, 444 U.S. 37, 42 (1979); see also *United States v. Morris*, 928 F.2d 504, 511 (2d Cir. 1991) (holding that the word “authorization” for purposes of the CFAA is “of common usage, without any technical or ambiguous meaning,” and therefore the district court “was not obliged to instruct the jury on its meaning”). Authorization is defined as “the state of being authorized” and “authorize” as “to endorse, empower, justify, permit by or as if by some recognized or proper authority.” WEBSTER’S THIRD INT’L DICTIONARY, 146 (3d ed. 2002). As applied here, access to a protected computer is “authoriz[ed]” when it occurs with “permission.” *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1132–33 (9th Cir. 2009); *Pulte Homes, Inc. v. Laborers’ Int’l Union of N. Am.*, 648 F.3d 295, 303–04 (6th Cir. 2011) (“Commonly understood, then, a defendant who accesses a computer ‘without authorization’ does so without sanction or permission”).

The indictment, in turn, alleges that Defendant and Khattab members worked together to share information regarding how to effectively “hack” into—that is, access without permission—Twitter accounts that did not belong to them and seize them—take them over—for the purpose of spreading ISIS information on the Internet. See [161] at 11–12, ¶ 5. According to the allegations, the entire scheme was designed to avoid or delay having Khattab members’ own social media accounts suspended or

closed once the pro-ISIS information was disseminated on Twitter. *Id.* at 11, ¶ 4. For example, the indictment alleges:

On or about April 12, 2018, Co-Conspirator C member posted, in Arabic, on Social Media Application A, “seize [a Twitter account], it is better because [the account] stays with you longer.” He then posted instructions, via a video link, to register Hotmail accounts in order to gain unauthorized access to Twitter accounts and wrote, in Arabic, “this technique is only for the supporters of the Caliphate.

Id. at 12, ¶ 8(a).


Such allegations clearly amount to “unauthorized” access, and thus the CFAA is not unconstitutionally vague as applied to Defendant’s alleged conduct. As for Defendant’s argument that “no unauthorized access” occurred here, that factual question is reserved for trial. For each of these reasons, the Court denies Defendant’s motion to dismiss Counts 3, 4, 6, 8, and 10 on these bases.

IV. Conclusion

For the reasons explained above, the Court denies Defendant’s motion for a bill of particulars [339] and motions to dismiss on multiplicity grounds, [340], [341]. The Court also denies Defendant’s motions to dismiss, motion to quash, and motion to suppress [372] as untimely and in violation of this Court’s standing orders and Local Rule 7.1. Even if the motions did not fail on procedural grounds, the Court holds that these motions fail on substantive grounds. The Court grants the government’s *Santiago* motions, [305], [377].

Date: May 7, 2025

ENTERED:


John Robert Blakey
United States District Judge