UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

UNITED STATES OF AMERICA,

v. Case No. 8:24-cr-68-KKM-TGW

TIMOTHY BURKE,

Defendant.

ORDER

Congress enacted the Wiretap Act in 1968 to combat nefarious actors intercepting Americans' private communications. In this case, the government argues that it can prove a Wiretap Act violation solely by showing that a defendant intentionally acquired a communication using a device and that the many exceptions to the Wiretap Act are not elements of the crime but instead defenses to be raised by a criminal defendant. Significant First Amendment concerns arise if I were to adopt the government's theory. To cure this constitutional concern, I look to the statutory exceptions and conclude that the government must plead and prove two of them: that a defendant was not a "party to the communication" and that any electronic communication was not "readily accessible to the general public."

I. BACKGROUND

Among other offenses, a grand jury charged that Timothy Burke violated the Wiretap Act, 18 U.S.C. § 2511, by intentionally intercepting several livestreams and by disclosing them. Indictment (Doc. 1) (Counts 8–12) (interception); *id.* (Counts 13–14) (disclosure). Burke allegedly gained access to StreamCo-Net, a livestreaming platform, and intercepted video and audio streams transmitted through it by a multinational media company (Network #1) and a commercial broadcast television and radio network (Network #2). Indictment (Count 1) ¶¶ 8–9, 13, 15, 23i. Burke then downloaded these communications and disclosed some of them. *Id.* ¶¶ 23i–23j.

Burke first moved to dismiss the Wiretap Act counts because, among other reasons, they fail to state an offense. *See* First MTD (Doc. 64) at 8–13; *see also* FED. R. CRIM. P. 12(b)(3)(B)(v). On Burke's view, the indictment should allege that any communications were acquired without consent and any electronic communications were not "readily accessible to the general public." First MTD at 8–13; 18 U.S.C. §§ 2510(2), 2511(2)(d), (2)(g)(i). I denied Burke's first motion to dismiss. First Order at 13–30. The Fifth Circuit's holding in *United States v. McCann*, 465 F.2d 147, 162 (5th Cir. 1972),[1] that consent was

[1] The Eleventh Circuit adopted as binding precedent all decisions rendered by the United States Court of Appeals for the Fifth Circuit prior to September 30, 1981. *See Bonner v. City of Pritchard*, 661 F.2d 1206, 1207 (11th Cir. 1981) (en banc).

a defense to, not an element of, a Wiretap Act charge foreclosed Burke's argument as to "consent" and informed treatment of other statutory exceptions, *see* First Order at 16–19. The order likewise underscored that Congress set out the provisions at issue among a "host of statutory exceptions located in other subsections" from the main proscription. First Order at 21. I thus concluded that, as a matter of statutory interpretation, the government did not need to negate either exception in the indictment. *Id.* at 18, 27.

In the light of that ruling, Burke now moves to dismiss again. Burke argues that Counts Eight through Fourteen violate the First Amendment because the Wiretap Act, as interpreted, is impermissibly overbroad and facially prohibits vast swaths of First Amendment-protected conduct. Third MTD (Doc. 125).[2] The government opposes. Resp. (Doc. 138).

In the light of the thorny constitutional and interpretive issues raised by Burke's motion, I invited *amici curiae* to address three questions:

> 1) Whether a video that includes both a human voice and visual data transmitted over the internet is an electronic communication, a wire communication, or both, as defined by 18 U.S.C. § 2510.

[2] This is Burke's third attempt to dismiss Counts Eight through Fourteen. His second motion unsuccessfully argued that the counts were duplicitous. Second MTD (Doc. 97); Second Order (Doc. 111) (denying Burke's Second MTD). Burke filed an earlier version of the present motion, *see* (Doc. 119), but I struck that motion because it contained "significant misrepresentations and misquotations of supposedly pertinent case law and history," (Doc. 124), which Burke's counsel attributed to the use of artificial intelligence, *see* (Doc. 126) ¶ 9.

2) Whether 18 U.S.C. § 2511(1)(a) prohibits a person watching a video on an internet streaming platform or visiting a public-facing webpage, without considering any of the statutory exceptions. If so, whether this interception would be deemed lawful by an exception in 18 U.S.C. § 2511, including whether such a viewer would have consent or would be a "party to the communication," *id.* § 2511(2)(d). If not, why not.

3) Whether, to avoid the chilling of protected activity, the Free Speech Clause of the First Amendment requires the government, in some cases, to allege in the indictment and to negate at trial a statutory exception to a criminal offense. Specifically, whether the Free Speech Clause requires the government to negate the "readily accessible" statutory exception for electronic communications, 18 U.S.C. § 2511(2)(g)(i), when prosecuting an intentional interception of an electronic communication, *id.* § 2511(1)(a), and the statutory exceptions for "consent" and "a party to the communication," *id.* § 2511(2)(d), when prosecuting an intentional interception of an electronic or wire communication, *id.* § 2511(1)(a).

(Doc. 128) at 4–5.

With the benefit of the parties' and *amici*'s papers, I reexamine the offense of intentional interception of communications under the Wiretap Act, 18 U.S.C. § 2511(1), and conclude that treating the exceptions from liability for "parties to the communication" and for electronic communications "readily accessible to the general public" as elements cures any First Amendment concern.

II. LEGAL STANDARD

An indictment is "a plain, concise, and definite written statement of the essential facts constituting the offense charged." FED. R. CRIM. P. 7(c)(1). An "indictment is sufficient if it '(1) presents the essential elements of the charged offense, (2) notifies the accused of the charges to be defended against, and (3) enables the accused to rely upon a judgment under the indictment as a bar against double jeopardy for any subsequent prosecution for the same offense.'" *United States v. Woodruff*, 296 F.3d 1041, 1046 (11th Cir. 2002) (quoting *United States v. Steele*, 178 F.3d 1230, 1233–34 (11th Cir. 1999)).

A defendant may move to dismiss an indictment that fails to state an offense. *See* FED. R. CRIM. P. 12(b)(3)(B)(v). "In judging the sufficiency of the indictment, the court must look to the allegations and, taking the allegations to be true, determine whether a criminal offense has been stated." *United States v. Fitapelli*, 786 F.2d 1461, 1463 (11th Cir. 1986). An indictment states an offense when it "allege[s] each of the elements of the statute." *United States v. Plummer*, 221 F.3d 1298, 1302 (11th Cir. 2000). "It is generally sufficient that an indictment set forth the offense in the words of the statute itself, as long as 'those words of themselves fully, directly, and expressly, without any uncertainty or ambiguity, set forth all the elements necessary to constitute the offence intended to be punished.'" *Hamling v. United States*, 418 U.S. 87, 117 (1974) (quoting *United States v. Carll*, 105 U.S. 611, 612 (1881)).

III. ANALYSIS

Burke argues that, as interpreted, the Wiretap Act violates the First Amendment. *See generally* Third MTD. While Burke earlier argued that the "consent" and "readily accessible to the general public" exceptions should be treated as elements, Burke never contended that the First Amendment required that reading. (Doc. 90) at 8. In the light of these new arguments and the *amici*'s submissions, the proper course is to consider (1) whether the offense of interception of a communication under the Wiretap Act creates a First Amendment issue, and (2) whether any exception must be considered an element to cure that concern.

As an antecedent matter, I encouraged the parties and *amici* to address whether the livestreams that Burke allegedly intercepted were "an electronic communication, a wire communication, or both." (Doc. 128) at 4. Contrary to the government's position in a recent hearing, *see* Hr'g Tr. (Doc. 135) 30:2–31:3, livestreams appear to be best understood as electronic communications, not a mixture of wire and electronic communications broken apart into the human voice and video aspects. In *United States v. Herring*, the Eleventh Circuit concluded that "satellite television signals" fell within the Wiretap Act's "very broad" definition of electronic communications. 993 F.2d 784, 785, 787 (11th Cir. 1993) (en banc). No basis appears for distinguishing the livestreams here from the satellite television signals in *Herring*. Both include video and audio

components. *See* Indictment (Counts 8–12) ¶¶ 2; *cf. Comark Commc'ns, Inc. v. Harris Corp.*, 156 F.3d 1182, 1183 (Fed. Cir. 1998) ("Conventional television signals contain two primary components: the video portion of the signal and the audio portion."). *See generally* Electronic Privacy Information Center (EPIC) Br. (Doc. 143) at 8–17.

I need not decide which kind of communication a livestream is to resolve this motion, though. Reading the exception for "parties to the communication" to be an element cures most First Amendment concerns because that exception applies to any communication—wire, oral, or electronic. And reading the exception for electronic communications that are "readily accessible to the general public" as an element doubly cures any constitutional problem.

A. If None of the Wiretap Act Exceptions are Elements, the Offense of Intentional Interception of a Communication Raises Serious First Amendment Concerns

If the Wiretap Act permits the investigation and prosecution of the intentional acquisition of *any* communication—full stop—then it raises serious First Amendment concerns under binding precedent. Burke and most of the *amici* contend that this is what the statute does if all its exceptions are defenses rather than elements. Third MTD at 5–10; ACLU Br. (Doc. 145) at 6–7, 12–22; Reporters Committee for Freedom of the Press Br. (Doc. 146) at 13–15; Internet Accountability Project (IAP) Br. (Doc. 158) at 15–16. I agree.

Without considering the statutory exceptions, the Wiretap Act prohibits "intentionally intercept[ing] . . . any wire, oral, or electronic communication." 18 U.S.C. § 2511(1)(a). The statute defines "intercept" to mean "acquire" using a device. *Id.* § 2510(4) (" '[I]ntercept' means the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."). And "acquire" in 1968 simply meant to "obtain" or "come to possess." *See Acquire*, WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 18 (1968) ("[T]o come into possession, control, or power of disposal of"); *Acquire*, THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 12 (1969) ("To gain possession of"); *see also Acquire*, THE RANDOM HOUSE DICTIONARY OF THE ENGLISH LANGUAGE 18 (2d ed. 1987) ("[T]o come into possession or ownership of; get as one's own"). To prove a Wiretap Act violation for intercepting a communication, then, the government would need to show only that the defendant intentionally acquired, using a device, the contents of a communication.

Significant First Amendment concerns arise if these are the only elements of a Wiretap Act interception offense.[3] *See Ashcroft v. Free Speech*

[3] Although the parties frame the First Amendment concern as arising under the Supreme Court's overbreadth doctrine, this action does not present an ordinary challenge of that kind. *See, e.g.*, *United States v. Williams*, 553 U.S. 285, 292 (2008) (explaining that under the "First Amendment overbreadth doctrine, a statute is facially invalid if it prohibits a substantial amount of protected speech" "relative to the statute's plainly legitimate sweep."); *Cheshire Bridge Holdings, LLC v. City of*

Coal., 535 U.S. 234, 255 (2002) ("The Government raises serious constitutional difficulties by seeking to impose on the defendant the burden of proving his speech is not unlawful."); *cf. Reno v. ACLU*, 521 U.S. 844, 881–82 (1997) (finding a defense inadequate to save a criminal statute from a First Amendment challenge). First, the government could bring to criminal trial anyone who intentionally acquires a communication—such as by accessing a webpage or streaming a YouTube video—even if he had a clearly applicable defense. *See Woodruff*, 296 F.3d at 1046 (explaining that an "indictment is sufficient if it '. . . presents the essential elements of the charged offense' "

Atlanta, 15 F.4th 1362, 1370–71 (11th Cir. 2021); *see also* Third MTD at 10 ("The statute is overbroad because it prohibits on its face all 'interceptions' not just those which are 'unlawful' or surreptitious."); Resp. at 3 ("The Court . . . should reject outright Burke's invitation to apply the overbreadth doctrine); *id.* at 24 ("Proper overbreadth analysis, at least of a 'bare' overbreadth challenge like Burke's . . . should be of both initial prohibition and exceptions to liability."). Burke does not argue, for example, that the Wiretap Act would allow the government to secure convictions for swaths of First Amendment-protected conduct, even if the First Amendment does not protect the conduct in which Burke allegedly engaged. *See* First Order at 6–13. Instead, the First Amendment concerns at play here require more of a constitutional avoidance analysis: in the light of the need to assign the burden of proof to a particular party in a criminal case, I must interpret what is an element and what is a defense. And I must do so consistent with long-standing precedent that instructs that Congress enacts statutes in conformity with the Constitution. *See, e.g.*, *United States v. X-Citement Video, Inc.*, 513 U.S. 64, 73 (1994). To be sure, the government never contends that Congress may, consistent with the First Amendment, give a person the burden of proving that his speech is lawful. I note though, if this case did require a true overbreadth doctrine inquiry, that test's pedigree is suspect as an original matter. *See, e.g.*, *United States v. Hansen*, 599 U.S. 762, 785 (2023) (Thomas, J., concurring) ("[The overbreadth] doctrine 'lacks any basis in the text or history of the First Amendment, relaxes the traditional standard for facial challenges,' and distorts the judicial role." (quoting *United States v. Sineneng-Smith*, 590 U.S. 371, 390 (2020) (Thomas, J., concurring))); *Moody v. NetChoice, LLC*, 603 U.S. 707, 752–66 (2024) (Thomas, J., concurring).

(quoting *Steele*, 178 F.3d at 1233–34)); *United States v. Salman*, 378 F.3d 1266, 1268 (11th Cir. 2004) (per curiam) ("Because [the defendant] was properly indicted, the government is entitled to present its evidence at trial."). It is "a fundamental aim of the First Amendment" to ensure that "the public has access to a wide range of views." *Moody v. NetChoice, LLC*, 603 U.S. 707, 741 (2024). Yet threatened with the Damoclean sword of prosecution for accessing unpopular speech, the public may choose to forgo hearing those views rather than "risk the perils of trial. There is a potential for extraordinary harm and a serious chill upon protected speech." *Ashcroft v. ACLU*, 542 U.S. 656, 670–71 (2004). Nor is this only a historical concern, as recent memory confirms that the federal government, at times, seeks to suppress disfavored views. *See Murthy v. Missouri*, 603 U.S. 43, 51–53 (2024) (detailing efforts by the White House, Surgeon General, CDC, and FBI to pressure social media companies to censor COVID-19 and election-related "misinformation").

Second, the government could use Wiretap Act violations as a basis for invasive search warrants. The potential availability of a defense does not negate probable cause (unless, perhaps, the government knows conclusively that the defense applies). *See, e.g.*, *Paez v. Mulvey*, 915 F.3d 1276, 1286 (11th Cir. 2019) ("[A]n affirmative defense to an alleged crime does not necessarily vitiate probable cause."); *Hall v. Trochessett*, 105 F.4th 335, 342 (5th Cir. 2024) ("A defense that may be raised in future proceedings does not vitiate probable

cause at the time of arrest."). Evidence of the mere acquisition of a communication might provide probable cause to search someone's email, text messages, video calls, or internet browsing history, chilling speech of all varieties. As some *amici* point out, this is no hypothetical danger. *See, e.g.*, ACLU Br. at 19–21 ("Journalists may not yet have been prosecuted for watching YouTube, but some recent cases are not far off."); Reporters Committee Br. at 11–13 (describing a 2023 raid on the offices of the Marion County Recorder and a reporter's home based on the reporter "accessing a state website and acquiring information that was meant to be publicly available" (citing Sofia Andrade & Paul Farhi, *After a Police Raid on a Kansas Newspaper, Questions Mount*, WASH. POST (Aug. 13, 2023), https://perma.cc/NCJ3-DVFY)).

The government and one *amicus* respond that the plain meaning of the Wiretap Act, even without any exceptions, does not allow for this parade of First Amendment horribles. They offer different reasons, but I part ways with both.

1. The Government's Ordinary Course of Business Argument

The government argues that there is no First Amendment problem because the Wiretap Act exempts interceptions by a device used "in the ordinary course of business." Resp. at 12 (quoting 18 U.S.C. § 2510(5)(a)). I

disagree with the government's reading of the statute, but even if correct, that provision does not allay the First Amendment concerns outlined above.

To cure the looming First Amendment problem, the government leans on a definition: the interception must be "by a device being used not 'in the ordinary course of business.' " *Id.* at 12 (quoting 18 U.S.C. § 2510(5)(a)). The statute explains that the interception of a communication must be "through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). As relevant here, the statute excludes from these kinds of "devices":

> any telephone or telegraph instrument, equipment or facility, or any component thereof, (i) furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business and being used by the subscriber or user in the ordinary course of its business or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business; or (ii) being used by a provider of wire or electronic communication service in the ordinary course of its business.

Id. § 2510(5)(a). In the government's view, this provision "neatly separates intentional from inadvertent wiretapping" by excluding from liability anyone using the device "in the ordinary course of business." Resp. at 8.

The government vastly overreads this exception. Critically, the statute does not except *all* devices used in the ordinary course of business, but only "any *telephone or telegraph* instrument, equipment or facility, or any component thereof . . . used in the ordinary course of its business." 18 U.S.C. § 2510(5)(a) (emphasis added). The government never explains why desktops,

laptops, smartwatches, smart TVs, Bluetooth speakers, or many of the other technologies that Americans use to acquire communications are "telephone or telegraph instrument[s], equipment or facilit[ies], or . . . component[s] thereof." *Id.* A modern smartphone might be within the semantic range of "telephone," *id.*, though that is doubtful given that Congress added the term in 1968, *see* Omnibus Crime Control and Safe Streets Act of 1968, Pub L. No. 90-351, § 802, 82 Stat. 197, 212; *see also Telephone*, WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 2350 (1968) ("An instrument for reproducing sounds esp. articulate speech at a distance"); *Telephone*, THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 1323 (1969) ("An instrument that directly modulates carrier waves with voice or other acoustic source signals to be transmitted to remote locations and that directly reconverts received waves into audible signals; especially, such an instrument connected to others by wire"). But many devices that people daily use to acquire communications fall outside the government's carveout.

The cases that the government cites do not alter the conclusion that "telephone or telegraph" cabins the reach of exempted devices. The government's in-circuit authority deals with the ordinary-course-of-business exception in the context of traditional telephony alone, not modern electronic communications. *See Watkins v. L.M. Berry & Co.*, 704 F.2d 577, 582–84 (11th Cir. 1983) (employer interception of employee's telephone call); *Simpson v.*

Simpson, 490 F.2d 803, 804, 809 & n.17 (5th Cir. 1974) (husband intercepting wife's telephone calls), *overruled by Glazner v. Glazner*, 347 F.3d 1212 (11th Cir. 2003) (en banc).

The government also relies on *Hall v. EarthLink Network, Inc.*, 396 F.3d 500, 503–05 (2d Cir. 2005), but that opinion is unpersuasive. The Second Circuit held that the ordinary-course-of-business exception applies to an interception by any "equipment or facility," not just those associated with telephones or telegraphs. *Id.* *Hall* reasoned that whether "telephone or telegraph" modify the whole series or just "instrument" was ambiguous and therefore relied on legislative history to favor the latter interpretation. *Id.* at 504. That reading is wrong. No ambiguity arises as "telephone or telegraph" clearly modify the parallel clauses that follow. *See* ANTONIN SCALIA & BRYAN A. GARNER, READING LAW: THE INTERPRETATION OF LEGAL TEXTS § 19, at 147 (2012) (series-qualifier canon) ("When there is a straightforward, parallel construction that involves all nouns or verbs in a series, a prepositive or postpositive modifier normally applies to the entire series."); *ECB USA, Inc. v. Chubb Ins. Co. of N.J.*, 113 F.4th 1312, 1322 (11th Cir. 2024), *cert. denied*, 145 S. Ct. 1431 (2025); *see also Facebook, Inc. v. Duguid*, 592 U.S. 395, 409–13 (2021) (Alito, J., concurring) (cautioning against overreliance on the series-qualifier canon but primarily addressing postpositive, not prepositive, modifiers). Nothing in the statute's text suggests otherwise, particularly as

Congress added the provision in 1968, long before the internet age, so there is no need to resort to legislative history. *See Wiersum v. U.S. Bank, N.A.*, 785 F.3d 483, 487–88 (11th Cir. 2015) ("Where the language of a statute is unambiguous, as it is here, we need not, and ought not, consider legislative history." (quoting *Harry v. Marchant*, 291 F.3d 767, 772 (11th Cir. 2002) (en banc))).

Even accepting the government's misreading as a permissible textual interpretation, the government's reliance on the ordinary-course-of-business exception to resolve any First Amendment problem is misplaced. The ordinary meaning of the phrase includes a business or commercial component, and the Fifth and Eleventh Circuits have always applied it in business or commercial contexts. *See Watkins*, 704 F.2d at 582 ("[T]he general rule seems to be that if the intercepted call was a business call, then [the company]'s monitoring of it was in the ordinary course of business. If it was a personal call, the monitoring was probably, but not certainly, *not* in the ordinary course of business."); *Briggs v. Am. Air Filter Co., Inc.*, 630 F.2d 414, 420 (5th Cir. 1980) ([T]he 'ordinary course of business' exception does not encompass interceptions not reasonably related to a business purpose."); *see also Royal Health Care Servs., Inc. v. Jefferson-Pilot Life Ins. Co.*, 924 F.2d 215, 216–19 (11th Cir. 1991) (per curiam) (interpreting identical language in the Florida Security of Communications Act, 934.02(4)(a)1., Fla. Stat.); *Epps v. St. Mary's Hosp. of Athens, Inc.*, 802

F.2d 412, 416–17 (11th Cir. 1986); *Ordinary Course of Business*, BLACK'S LAW DICTIONARY (4th rev. ed. 1968) ("The transaction of business according to the usages and customs of the commercial world generally or of the particular community or (in some cases) of the particular individual whose acts are under consideration"); *Ordinary Course of Business*, BLACK'S LAW DICTIONARY (6th ed. 1990) (similar). The government provides no authority suggesting that the ordinary-course-of-business exception protects purely private, noncommercial conduct like watching a YouTube video or accessing an online article.

The government has thus not shown that an exception to the definition of "device" ameliorates the First Amendment concern.

2. The Government's Argument about the Scope of the Wiretap Act's Chilling Effect

The government argues at length that "[t]he wiretap statute does not chill hearing or listening to (or watching) anything" but merely prohibits *acquiring* a communication. Resp. at 13–23; *see id.* at 17–18 (arguing that the Wiretap Act "cannot even be interpreted to prohibit, as an illegal wiretap, the 'listening' or 'viewing' anything" because "the human ear or eye is not a 'device' " and "no ear or eye 'acquires' a communication as necessary to trigger the wiretap statute"). In other words, the government contends that the Wiretap Act creates no First Amendment problem because, while it might prohibit digitally accessing an article, it does not prohibit reading it.

The absurdity of this position is plain. "The right of freedom of speech and press . . . embraces the right to distribute literature and necessarily protects the right to receive it." *TikTok Inc. v. Garland*, 604 U.S. 56, 69 (2025) (quoting *Martin v. City of Struthers*, 319 U.S. 141, 143 (1943)). Were the government right, a regulation that prohibited members of the public from taking flyers on a matter of public concern—but permitted offering the flyers and reading them—would pass constitutional muster. That is not the law.

The government does try to moderate its extreme position. First, it maintains that the Wiretap Act does not regulate " 'streaming' anything" because streaming is not "an intentional acquisition by *unauthorized device*." Resp. at 19 (emphasis added). As explained above, the government's construction of what constitute "unauthorized devices" is at odds with the statute's text. Second, the government contends that "the subscriber or user of an online electronic communication service, who is hearing, listening, watching a program, or streaming—'accessing online' entertainment content—also does not have the requisite mens rea for an illegal wiretap." *Id.* Yet if all the government need prove to secure a conviction is that a person "intentionally" acquires a communication using a device that is not so. 18 U.S.C. § 2511(1)(a). One can intentionally obtain a communication with no other nefarious or unlawful intent and still fall within the ambit of the Wiretap Act as facially defined.

The government's argument that no First Amendment problem exists because "[t]he Constitution does not provide Burke the right to *take* others' private and proprietary information" is therefore without merit. Resp. at 21. The question at this stage is not whether Congress may lawfully prohibit Burke's particular alleged conduct—it may. The question is whether the statute's structure raises serious First Amendment concerns—it does. And the government's statutory interpretation arguments fail to mitigate those concerns.

The government thus fails to show that, bracketing the Wiretap Act's exceptions, the Act does not prohibit First Amendment-protected conduct.

3. *Amicus* Internet Accountability Project's Ordinary Meaning of "Intercept" Argument

Amicus Internet Accountability Project proposes to cure any First Amendment concern by reading "intercept" in accord with its narrower, ordinary meaning, rather than its broad statutory definition. *See* IAP Br. at 9–13. In the alternative, Internet Accountability argues that both the "party to a communication" and "readily accessible to the general public" exceptions must be treated as elements to remedy any First Amendment concern. I agree with Internet Accountability's alternative argument and explain why later, but first address why I am compelled to read "intercept" consistent with its broad statutory definition.

Recall, the Wiretap Act defines "intercept" to mean roughly "to acquire using a device," 18 U.S.C. § 2510(4), while intercept's ordinary meaning is "[t]o stop, deflect, or interrupt the progress or intended course of" something, *Intercept*, THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 683 (1969); *see also Intercept*, WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 1176 (1968) ("[T]o take, seize, or stop by the way or before arrival at the destined place" or to "stop or interrupt the progress or course of"); *Intercept*, THE RANDOM HOUSE DICTIONARY OF THE ENGLISH LANGUAGE 992 (2d ed. 1987) ("[T]o stop or interrupt the course, progress, or transmission of" or "to see or overhear (a message, transmission, etc., meant for another)"). Using intercept's ordinary meaning, Internet Accountability argues that "only an unauthorized viewer can 'intercept,' " for example, "a video on the internet." IAP Br. at 9.

Absent patent ambiguity, a statutory definition is almost always conclusive of a statutory term's meaning. SCALIA & GARNER, READING LAW § 36, at 228 (interpretive-direction canon). When the definition itself contains an ambiguity though, the defined term's ordinary meaning might interpret an ambiguous definition. *See, e.g.*, *Delligatti v. United States*, 145 S. Ct. 797, 808–09 (2025); *Sackett v. EPA*, 598 U.S. 651, 672 (2023); *see also Van Buren v. United States*, 593 U.S. 374, 404 (2021) (Thomas, J., dissenting). But there must be some ambiguity—otherwise, departing from the statutory definition

is just "result-driven antitextualism." *Bond v. United States*, 572 U.S. 844, 868 (2014) (Scalia, J., concurring in the judgment); SCALIA & GARNER, READING LAW § 36, at 228 ("It is very rare that a defined meaning can be replaced with another permissible meaning of the word on the basis of other textual indications."). Here, the Wiretap Act defines "intercept" to mean, in essence, "acquire using a device." *See* 18 U.S.C. § 2510(4). No patent ambiguity there, and thus no basis to depart from Congress's definition.

Reading "intercept" in accord with its ordinary meaning instead of its statutory one also renders some of the Wiretap Act exceptions nullities. Internet Accountability stresses that a broad reading of "intercept" "would criminalize, at the federal level, an extraordinary amount of conduct." IAP Br. at 11. I would agree if Congress had not included the statutory exceptions. Unlike instances where backdrop "unexpressed presumptions" might favor a different meaning, Congress included explicit limits on the extent of criminal liability in the very text of the statute: as exceptions. *Bond*, 572 U.S. at 857. Jettisoning the statutory definition for the ordinary meaning of "intercept" would render at least one of the exceptions—that parties to the communication are ordinarily not liable for acquisitions—superfluous. Someone cannot intercept in the colloquial sense a communication that he sent or that is intended for him. *See infra* at 25–26. Courts, of course, disfavor statutory readings that render another part of the statute "superfluous, void, or

insignificant." *Fuerst v. Hous. Auth. of Atlanta*, 38 F.4th 860, 869 (11th Cir. 2022) (quoting *In re Shek*, 947 F.3d 770, 777 (11th Cir. 2020)).

Because Internet Accountability's first proposed solution to the First Amendment problem is incompatible with the statute's plain meaning, I decline to adopt it.

* * *

Neither the government nor the *amici* offer a reason to interpret § 2511(1) in a way that does not facially sweep in swaths of First Amendment-protected conduct. If all the government must allege is that the defendant intentionally acquired a communication using a device, then the Wiretap Act raises serious First Amendment concerns. *See Ashcroft v. ACLU*, 542 U.S. at 670–71; *Free Speech Coal.*, 535 U.S. at 255. In such cases, "[c]ourts should . . . construe statutes 'to avoid not only the conclusion that they are unconstitutional, but also grave doubts upon that score.'" *United States v. Palomar-Santiago*, 593 U.S. 321, 328–29 (2021) (alteration adopted) (quoting *United States v. Jin Fuey Moy*, 241 U.S. 394, 401 (1916)); *see also* H.R. REP. NO. 99-647, at 39–40 (1986) (explaining that the Electronic Communications Privacy Act amended part of 18 U.S.C. § 2511(2)(d) to stymie "attempts by parties to chill the exercise of First Amendment rights," specifically "responsible news gathering"); S. REP. NO. 99-541, at 17–18 (1986) (same).

B. The "Party to the Communication" and "Readily Accessible" Exceptions Are Elements

Because the Wiretap Act does not unambiguously explain which of its provisions are elements and which are defenses, the presumption that Congress intends to legislate consistent with the First Amendment supports treating some exceptions to intentional interception of a communication as elements.

"Determining whether an exception in a criminal statute creates an element or an affirmative defense is not an exact science." *United States v. Rafiekian*, 991 F.3d 529, 541 (4th Cir. 2021). The heart of the inquiry is whether the offense can "be accurately and clearly described" without reference to the exception, or whether the exception is a key "ingredient[]" of the offense. *United States v. Cook*, 84 U.S. 168, 173–74 (1872); *see United States v. Outler*, 659 F.2d 1306, 1309 (5th Cir. Unit B Oct. 1981)[4] (holding that a part of a statute that "embodies the culpability of the offense" "is an essential element of [the] offense"). In this Circuit, courts look to three considerations to determine whether a statute defines an element or a defense: (1) "the language and structure of the statute"; (2) "the legislative history of the provision"; and (3) "whether the defendant or the government is better situated to adduce

[4] Decisions rendered by a Unit B panel of the former Fifth Circuit are considered binding precedent in the Eleventh Circuit. *Stein v. Reynolds Sec., Inc.*, 667 F.2d 33, 34 (11th Cir. 1982).

evidence tending to prove or disprove the applicability of the exception." *United States v. McArthur*, 108 F.3d 1350, 1353 (11th Cir. 1997). The first consideration is, of course, the most important. *See United States v. Steele*, 147 F.3d 1316, 1318 (11th Cir. 1998) (en banc) ("In construing a statute we must begin, and often should end as well, with the language of the statute itself." (quoting *Merritt v. Dillard Paper Co.*, 120 F.3d 1181, 1185 (11th Cir. 1997))).

1. The Government Must Plead and Prove That Burke Was Not a "Party to the Communication" That He Allegedly Intercepted

The earlier order presented no occasion to address the party-to-the-communication exception, but I conclude now that the government must plead and prove it as an element. Beginning with the text, *see Groff v. DeJoy*, 600 U.S. 447, 468 (2023), the Wiretap Act provides broadly that

> any person who . . . intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . . shall be [subject to criminal punishment or civil action].

18 U.S.C. § 2511(1). The statute includes over twenty exceptions (depending on how you count them) from that sweeping prohibition, including acquiring a communication to which one is a party:

> It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where *such person is a party to the communication* or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious

> act in violation of the Constitution or laws of the United States or of any State.

Id. § 2511(2)(d) (emphasis added).

Narrow provisos to broad proscriptions ordinarily set out defenses, not elements. That is the Supreme Court's long-settled rule, one recognized in this Circuit. *See McKelvey v. United States*, 260 U.S. 353, 357 (1922) ("[A]n indictment . . . founded on a general provision defining the elements of an offense . . . need not negative the matter of an exception made by a proviso or other distinct clause, whether in the same section or elsewhere."); *McArthur*, 108 F.3d at 1353 ("[A] narrow proviso to a more general statutory offense is more likely to be an affirmative defense than an element of the offense."). Like other background principles of interpretation, courts assume that Congress writes with this general rule in mind absent "compelling reason to think" otherwise. *Meacham v. Knolls Atomic Power Lab'y*, 554 U.S. 84, 91 (2008).

Two "compelling reason[s]" teach that the Wiretap Act does not follow, at least in part, that general rule: (1) serious First Amendment concerns counsel against a broad interpretation of the core offense, *see supra* at 7–21, and (2) the use of "intercept" to define the offense suggests that more than the mere acquisition of an electronic communication is at the offense's heart.

To start, reading the party-to-the-communication exception as an element ameliorates most of the First Amendment concerns identified above

and discussed by the parties and *amici*. Many of the examples that Burke and the *amici* provide involve someone acquiring electronic data from the internet, like accessing The Wall Street Journal or TikTok or streaming a YouTube video. *See, e.g.*, Third MTD at 2, 7, 15; ACLU Br. at 1, 10. For ordinary public videos and webpages, the acquiror will be a party to the communication: the intended recipient of data sent from the website's server. *See United States v. Tagg*, 886 F.3d 579, 583 n.2 (6th Cir. 2018) ("Anytime you click on a website's content (e.g., a link, an image, a page), the website's host computer transmits data to your computer, allowing you to view the content that you requested."); *cf. In re Google Inc. Cookie Placement Consumer Priv. Litig.*, 806 F.3d 125, 140–45 (3d Cir. 2015) ("[T]he intended recipient of a communication is necessarily one of its parties, and the defendants were the intended recipients of the . . . requests they acquired here, [so] the defendants were parties to the transmissions at issue in this case."). The statute thus would not facially prohibit most of the acquisitions about which Burke and the *amici* are concerned.

The ordinary meaning of "intercept" also supports reading the party-to-the-communication exception as an element. Using the word "intercept" in the core offense language suggests that the acquiror must not be a party to the communication. In everyday language, to "intercept" means "[t]o stop, deflect, or interrupt the progress or intended course of" something. *Intercept*, THE

AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 683 (1969); *Intercept*, WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 1176 (1968); *see United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003); *see also Intercept*, THE RANDOM HOUSE DICTIONARY OF THE ENGLISH LANGUAGE 992 (2d ed. 1987) ("to stop or interrupt the course, progress, or transmission of" or "to see or overhear (a message, transmission, etc., meant for another)").[5] These definitions suggest that for one to intercept a communication, the communication must (1) be acquired during its transit between an origin and a destination, and (2) be acquired by someone who is neither the sender nor the intended recipient. *See Steiger*, 318 F.3d at 1048–49 ("[A] contemporaneous interception—*i.e.*, an acquisition during 'flight'—is required to implicate the Wiretap Act with respect to electronic communications.").

The use of "intercept" in the principal subsection that proscribes the conduct is indicative of the "definition of the offense" Congress created through § 2511(1). *United States v. Kloess*, 251 F.3d 941, 945 (11th Cir. 2001). Congress could have chosen any number of words with a similar meaning to "acquire" to denote the actus reus—"obtain," or "procure," for example. It would be surprising for Congress to choose the word "intercept" as the principal term setting out the offense conduct while nevertheless intending the offense to be

[5] The legal definition of "intercept" is that provided by the Wiretap Act. *See Intercept*, BLACK'S LAW DICTIONARY (5th ed. 1979) (citing 18 U.S.C. § 2510).

far, far broader. *Cf. Delligatti*, 145 S. Ct. at 810 ("Since on this side of the looking-glass an entirely artificial definition is rare, the meaning of the definition is almost always closely related to the ordinary meaning of the word being defined." (quoting SCALIA & GARNER, READING LAW at 228)). Given the term's ordinary meaning and in context, "intercept" suggests prohibition of only a third-party acquisition of a communication during transmission, even if the Act achieves that goal in part through its exceptions and not exclusively through § 2511(1). The Eleventh Circuit has already recognized the "during transmission" component of the offense. *See Steiger*, 318 F.3d at 1048–49. Reading the party-to-the-communication exception as an element gives effect to the "third-party" component of "intercept."

The best reading of the Wiretap Act's text thus suggests that it is an "essential element of the offense" that the acquiror not be a "party to the communication." 18 U.S.C. § 2511(2)(d); *Outler*, 659 F.2d at 1309.[6]

[6] In many ways, I agree with Internet Accountability's first argument that the term "intercept" does important work in the Wiretap Act's overall meaning, but I differ on the way in which it manifests. By adhering to the statutory definition of "intercept," I need not render the party-to-the-communication exception and the statutory definition nullities. Instead, the ordinary meaning of "intercept" informs a question that the statute does not answer expressly: what are the elements of this offense? In doing so, it gives effect both to the statutory definition of "intercept" and all the exceptions, while also respecting Congress's choice of the word "intercept" to describe the offense conduct.

"[T]he 'legislative history of the provision' " "provides little additional insight." First Order at 22 (quoting *McArthur*, 108 F.3d at 1353). The broad purpose of the Wiretap Act—to protect privacy while allowing adequate law-enforcement information gathering—is well established. *See* Omnibus Crime Control and Safe Streets Act § 801 (findings). The committee reports' commentary on the party-to-the-communication exception is uninstructive. The 1968 act's Senate Report states merely that the act included the exception for parties to the communication in 18 U.S.C. § 2511(2)(d)[7] because it "largely reflects existing law." S. REP. NO. 90-1097, at 93–94 (1968). Both the House and Senate Reports for the Electronic Communication Privacy Act (ECPA), which extended the Wiretap Act to electronic communications, *see* Pub. L. No. 99-508, § 101, 100 Stat. 1848, 1848–53 (1986), discuss an amendment to § 2511(2)(d) striking the language "or for the purpose of committing any other injurious act," which followed the carveout for interceptions in furtherance of criminal or tortious acts. *See* H.R. REP. NO. 99-647, at 39–40; S. REP. NO. 99-541, at 17–18. While the reports explain that the change was motivated by concern about journalists' First Amendment rights,[8] they do not shed any light

[7] Section 2511(2)(c) in the version reported out of the Senate Committee on the Judiciary. *See* S. REP. NO. 90-1097, at 12 (1968).

[8] The reports both express concern with the Sixth Circuit's decision in *Boddie v. American Broadcasting Companies, Inc.*, 731 F.2d 333 (6th Cir. 1984). *See* H.R. REP. NO. 99-647, at 39–40; S. REP. NO. 99-541, at 17–18. In *Boddie*, in which ABC

on whether the party-to-the-communication exception is an element or an affirmative defense.

As in the previous order, "I agree that, in the ordinary case, 'a defendant will be in the best position to prove facts necessary' to establish that" he was a party to the communication at issue. First Order at 23. This is unsurprising; the defendant is ordinarily "the most knowledgeable and unimpeachable source of information about his past conduct." *Bruton v. United States*, 391 U.S. 123, 140 (1968) (White, J., dissenting). While this factor favors treating the party-to-the-communication exception as a defense, I give it minimal weight because that is likely true in most criminal contexts.

The earlier order concluded that *United States v. McCann*'s holding that the consent exception was a defense applied equally to the "readily accessible" exception. First Order at 19 (reasoning "that exceptions in the same statutory clause should be 'treated similarly' " (quoting *United States v. Haggerty*, 997 F.3d 292, 300–01 (5th Cir. 2021))); *see also* 18 U.S.C. §§ 2510, 2511(2) (creating over twenty exceptions to § 2511(1)). Without the free speech concerns, the

---

journalists had surreptitiously recorded an interview, the Sixth Circuit held that whether the journalists recorded the interview "with a 'purpose of committing any other injurious act' " was for the jury because the plaintiff claimed "that the [journalists'] purpose was 'to cause the Plaintiff insult and injury.' " 731 F.3d at 336–38. In the committees' view, "[t]his interpretation of the statute places stumbling blocks in the path of even the most scrupulous journalist" and is "inconsistent with the guarantees of the First Amendment." H.R. REP. NO. 99-647, at 39–40; *see* S. REP. NO. 99-541, at 17. This shows a concern about the First Amendment implications of the Wiretap Act, but it does not clarify what constitutes the elements of the offense.

order relied on binding precedent treating one statutory exception as a defense to imply that similar statutory exceptions also are best read as defenses. I also gave great weight to the statutory structure of the Wiretap Act, which proscribes the primary conduct in the first subsection and then enumerates around twenty exceptions in later subsections and definition sections. While that structure remains and *McCann* no doubt supports the prior order's conclusion, it does not require that all statutory exceptions must be treated as defenses.

First, *McCann* addressed only the consent exception, and only briefly. The Fifth Circuit at first characterized the defendants' argument as "that the [trial] court committed reversible error by not dismissing the indictment against the [defendants] because it did not negate *all* the statutory exceptions listed in 18 U.S.C. § 2511." *McCann*, 465 F.2d at 162 (emphasis added). Yet the court answered the defendants' argument by saying that "[i]t was not necessary to recite in the indictment that the interceptions were made without consent. If the appellants believed that they came within the consent exception it was incumbent upon them to prove this fact." *Id.*; *see also id.* ("[A]s will be discussed later, it was not necessary that the Government prove that no party to the conversations which were intercepted consented to their interception."). While a "decision can hold nothing beyond the facts of [the] case" no matter "what a court says in its opinion," *Edwards v. Prime, Inc.*, 602 F.3d 1276, 1298

(11th Cir. 2010), nothing in the *McCann* opinion attempts to resolve whether the other exceptions are defenses or elements.

Second, the Eleventh Circuit did not address or follow *McCann* in *Snow v. DirecTV*, 450 F.3d 1314 (11th Cir. 2006). There, the Eleventh Circuit concluded, though in a civil context and under the Stored Communications Act (SCA),[9] that "the requirement that the electronic communication not be readily accessible by the general public is material and essential to recovery under the SCA." *Id.* at 1321. To hold otherwise would, the court said, subject "the merely curious" to prosecution. *Id.* To be sure, the SCA contains no party-to-the-communication provision like the Wiretap Act, as that statute addresses access to electronically stored information, so the Eleventh Circuit had no occasion to cure any First Amendment concern through that exception. But its concern carries over to this context too. While *Snow* did not cite *McCann*, its interpretation of the same provision—18 U.S.C. § 2511(2)—in a closely related context suggests that *McCann*'s reasoning does not extend to every exception in § 2511.

Third, the *McCann*'s treatment of "consent" as a defense is consistent with the ordinary meaning of "intercept." Someone may still intercept a communication even if they have permission to do so. *See Intercept*, THE

[9] Congress enacted the Stored Communications Act as Title II of the ECPA, §§ 201–02, 100 Stat. at 1860–68.

AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 683 (1969); *Intercept*, WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 1176 (1968); *Steiger*, 318 F.3d at 1048–49. For example, it is perfectly natural to say that a law enforcement officer who taps a phoneline with the consent of the confidential informant using that line is "intercepting" calls made from third parties to the informant.

McCann thus does not foreclose treating the party-to-the-communication exception as an element.

The Wiretap Act's text and significant First Amendment concerns support treating the party-to-the-communication exception as an element that the government must plead and prove. The legislative history is neutral, and the "ease of proof" weighs weakly toward treating it as a defense. And precedent does not dictate the outcome. On balance, I conclude that it is an element.

2. The Government Must Also Plead and Prove that Any Electronic Communications Were Not "Readily Accessible to the General Public"

In the light of the above reasons supporting that the party-to-the-communication exception is an element, I conclude that the readily-accessible-to-the-general-public exception for electronic communications is also an element. Three reasons support that conclusion.

First, the readily accessible exception for electronic communications cures the Wiretap Act's potential First Amendment problems. The parties did not raise any First Amendment concerns in the briefing on Burke's first motion to dismiss, other than Burke's argument that Counts Thirteen and Fourteen violated *Bartnicki v. Vopper*, 532 U.S. 514 (2001). *See* First Order at 6–13. Yet the readily accessible exception addresses the First Amendment concerns that Burke raises now in much the same way that the party-to-the-communication exception does.

> Section 2511(g)(i) provides that a person may lawfully
>
> > intercept or access an electronic communication made through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public.

An "electronic communication system" means, generally, "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications." 18 U.S.C. § 2510(15). The readily accessible exception thus precludes liability for intercepting electronic communications that most ordinary Americans can access, regardless of whether they are parties to the communication in question.

The majority of feared chilled speech involves a casual internet user mostly accessing websites or applications—Instagram, X, Netflix, The Washington Post—that are readily accessible to the public. These websites are

configured to be accessible to people equipped with today's standard technology and plainly fall within the exception's ambit. Making the readily accessible exception an element removes the ordinary user's protected access to speech from the statute's sweep.

Second, *Snow* counsels strongly in favor of treating the readily accessible exception as an element. *Snow* concluded that, in the context of an SCA civil action, a valid complaint must allege that the "the electronic communication not be readily accessible by the general public." 450 F.3d at 1321. While *Snow* did not cite the First Amendment, it justified this holding mainly in terms of public access to information. *Id.* ("If by simply clicking a hypertext link, after ignoring an express warning, on an otherwise publicly accessible webpage, one is liable under the SCA, then the floodgates of litigation would open and the merely curious would be prosecuted. We find no intent by Congress to so permit.").

Neither *Snow* nor *McCann* control for purposes of determining who bears the burden of proof for the readily accessible exception but the two cases cut against one another. *See* First Order at 26–27. But in the light of the First Amendment concerns recently raised, *Snow* weighs heavily in favor of treating the readily accessible exception as an element in the criminal context.

Third, treating the party-to-the-communication exception differently than the readily accessible exception risks confusing the jury. Both exceptions

thrust at the same question—the nature of the defendant's access to the allegedly intercepted communication. Placing the burden for proving one exception on the government and the other on the defendant creates a significant risk of a jury confusion, particularly given the technological complexity of a case like this.

In the light of these considerations, I conclude that the government must plead and prove that any electronic communications that Burke allegedly intercepted were not readily accessible to the general public.[10]

C. Dismissal of the Indictment is the Appropriate Remedy

The government does not allege in the indictment that Burke was not a party to the communications or that the electronic communications that Burke allegedly intercepted were not readily accessible to the general public, so dismissal is the ordinary remedy. *See United States v. Martinez*, 800 F.3d 1293, 1295 (11th Cir. 2015) (per curiam). *Amicus* Internet Accountability contends that dismissal is unnecessary because the allegations in the indictment fairly

[10] Because the readily accessible exception is an element and applies only to the offense of intercepting electronic communications, intercepting wire and electronic communications have different elements and are therefore now different offenses, not merely different means of committing the same offense. *See Blockburger v. United States*, 284 U.S. 299, 304 (1932); *see also United States v. Burton*, 871 F.2d 1566, 1573 (11th Cir. 1989) (explaining that an indictment must charge distinct crimes in separate counts). If the United States elects to file a superseding indictment, it should consider this order's implications for the indictment's structure, as well as its conclusion that the livestreams Burke allegedly intercepted are likely electronic communications, not oral or wire. *See supra* at 6–7 (citing *Herring*, 993 F.2d at 785, 787).

imply that Burke was not a party to the communications and that the communications were not readily accessible. *See* IAP Br. at 21–23 (citing *Woodruff*, 296 F.3d at 1045–48). While I am inclined to agree as a matter of context, precedent suggests that best practice is for the indictment to track the language of the statute. *See United States v. Moore*, 954 F.3d 1322, 1332 (11th Cir. 2020). As there is minimal prejudice to requiring the government to supersede in this manner, particularly as a date certain for trial has yet to be set, *see* (Doc. 185), dismissal without prejudice of the Wiretap Act counts is appropriate.

IV. CONCLUSION

Burke raises significant First Amendment concerns if the Wiretap Act facially prohibits the mere acquisition of communications using a device. But reading the party-to-the-communication and readily accessible exceptions as elements of a Wiretap Act offense remedies those concerns. Because the indictment does not allege either with regards to Counts Eight through Fourteen, those counts are dismissed without prejudice.

This ruling leaves several potential paths forward for the government. First, the government may proceed to trial on the remaining counts in the current indictment and abandon the Wiretap Act counts. Second, the government may appeal this decision and postpone trial until the Eleventh Circuit clarifies the law regarding the Wiretap Act interception offenses. *See*

18 U.S.C. § 3731. Third, the government may supersede and cure the counts consistent with this order. I note that, given the parties' arguments and representations about the evidence, this last route would appear to minimally impact the parties' anticipated trial presentation. Burke does not dispute that he acquired the communications, but instead whether he did so consistent with the Wiretap Act exceptions. The government's arguments (and I assume evidence) are that he did not. So although this order shifts the burden of proof on those exceptions, it does not alter the focus of the trial.

Accordingly, defendant Timothy Burke's Third Motion to Dismiss (Doc. 125) is **GRANTED**. Counts Eight through Fourteen of the Indictment (Doc. 1) are **DISMISSED without prejudice**.

ORDERED in Tampa, Florida, on September 25, 2025.

Kathryn Kimball Mizelle
United States District Judge