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

UNITED STATES' RESPONSE OPPOSING BURKE'S THIRD MOTION TO DISMISS

The United States opposes Burke's third motion to dismiss his indictment, *Defendant's Replacement Memorandum of Law in Support of Motion to Dismiss Counts 8, 9, 10, 11, 12, 13, and 14* (Doc. 125; hereafter, "Motion"). Burke now challenges his indictment as brought pursuant to a fatally "overbroad" statute. The Motion engages in no textual analysis and presents no correct constitutional analysis. It fails.

I. Introduction

Burke is charged with illegal wiretapping, and knowingly disclosing the contents of his unlawfully obtained communications, in violation of 18 U.S.C. § 2511(1) (hereinafter the "wiretap statute"). Doc. 1. Having failed, under *McCann*, to convince this Court that the affirmative defenses he says he will raise at trial—prior consent to the otherwise illegal wiretap under § 2511(2)(d), and proof that the system he tapped was already configured to allow public access—are actually elements of a wiretapping crime, Burke takes a different tack: If the wiretap statute's

affirmative defenses are affirmative defenses, he says, then the statute itself is unconstitutionally "overbroad" under the First Amendment—it chills such a substantial portion of others' protected speech, relative to legitimately regulated conduct, that it cannot stand. *See* Doc. 125 at 5-8.

Burke "bears the burden of demonstrating, from the text of the law and from actual fact, that substantial overbreadth exists." *Virginia v. Hicks*, 539 U.S. 113, 122 (2003) (cleaned up). Yet he fails even to shoulder that burden. He simply asserts a parade of First Amendment horribles: The wiretap statute, he says, prohibits modern citizens from functioning lawfully in the Internet age—it criminalizes "merely access[ing] a streaming TikTok or YouTube video, a live stream, or any content containing the human voice, without first procuring a party's consent." Doc.125 at 4; it renders illegal "view[ing] and listen[ing] to each and every bit of information online," *id.* at 4–5; it prohibits "the download of any content containing the human voice," *id.* at 6.

This is nonsense; the statute does no such things. Congress designed the wiretap statute to ensure against government intrusion on the security and privacy of information in the telecommunications age, while still allowing appropriate government electronic surveillance. *See* S.Rep. 90-1097 at 47, 60-64. It designed the criminal portion of the statute to align private liability for wiretapping with law enforcement's prohibitions, preventing a person such as Burke from intentionally intercepting—that is, acquiring, by unauthorized device, both wire and electronic

communications in transit over interstate wires. *See Id.* at 2-3, 47, 60-64. The wiretap statute is essentially a theft statute—protecting against unauthorized acquisition the same interests/property interests protected by the Fourth Amendment against unreasonable governmental search and seizure—and it does not intrude on our First Amendment right to speak (or hear or watch) at all. Indeed, it is Burke's alleged intentional wiretapping of proprietary audio/video streams containing internal media outlet deliberations, perusing those feeds, and then using them as he sees fit, that deters conduct covered under the First Amendment.

But even if Burke were correct that the wiretap statute regulates speech, his overbreadth analysis is flawed—indeed, nonexistent. He does not establish that the statute chills the "substantial" amount of speech it must to fail. He does not explain his "conversion" theory (if affirmative defenses were converted to elements, the statute would fare better): He explains neither why a reviewing court must blind itself to statutory exceptions when considering overbreadth nor why converting the burden of proof for the exceptions he wishes to raise at trial would solve overbreadth.

This Court need not revisit its decision under *McCann*. It should reject outright Burke's invitation to apply the overbreadth doctrine. Striking a statute for overbreadth is "strong medicine," always employed "with hesitation, and then only as a last resort," *New York v. Ferber*, 458 U.S. 747, 769 (1982) (cleaned up)—and here, it is completely unwarranted.

II. Summary of Argument

At the May 6 and 20 hearings, this Court asked the United States to elucidate its position regarding Burke's (ill-defined) potential overbreadth challenge by explaining: (1) What conduct the wiretap statute prohibits (and whether Burke's alleged conduct is illegal wiretapping of both "wire" and "electronic" communications under the statute); (2) Whether, by criminalizing intentional wiretapping of interstate communications facilities, Congress has impermissibly burdened Freedom of Speech for us all—and, if so, whether shifting the burden of proof at trial for Burke's planned factual defenses will solve the problem; and (3) Whether, if the wiretap statute is unconstitutionally overbroad and would not be so were its statutory exceptions elements of Burke's crimes, this Court should revisit its prior decision under *McMann*. *See* Doc. 135 at 17, 24-29, 32-34; Doc. 136 at 6-8, 16-17; *see also* Doc. 128 at 4-5. As the Court summed up: "[I]f it is that the elements [of the crime] are [merely] the interception of an electronic or wire communication, how do those not create an affront to the First Amendment particularly chilling core protected speech?" Doc.136 at 7; *see also* Doc. 128 at 4-5 (Court's invitation to non-parties to advocate for or against Burke's constitutional defense).

The United States responds as follows: (1) The wiretap statute prohibits the intentional acquisition, by a device used not "in the ordinary course of business," of a defined communication (and, as charged, Burke acquired both "wire" and "electronic" communications when he tapped into StreamCo's audio/video

streams); (2) The statute therefore does not implicate First Amendment conduct and does not burden our Freedom of Speech at all, let alone by chilling a substantial portion of protected speech in relation to the unprotected speech it regulates—and regardless, Burke's "conversion" theory lacks support; and (3) This Court therefore should not revisit its previous decision under *McCann*.

III. Argument

A. Burke's implication throughout his Motion—that the wiretap statute regulates speech—is wrong, according to the text of the statute.

i. The wiretap statute prohibits the intentional acquisition, by a device being used not "in the ordinary course of business," of a communication in transit over interstate communication facilities.

The "first task" when considering an overbreadth challenge "is to determine whether the enactment reaches a substantial amount of constitutionally protected conduct." *Vill. of Hoffman Ests. v. Flipside, Hoffman Ests., Inc.*, 455 U.S. 489, 494 (1982). Thus, "[t]he first step" in that first task, "is to construe the challenged statute; it is impossible to determine whether a statute reaches too far without first knowing what the statute covers." *United States v. Williams*, 553 U.S. 285, 293 (2008). We therefore start with the plain language of the statute.

As relevant to the charged conduct, when Burke tapped StreamCo's audio/video streams, § 2511(1)(a) prohibited him from, "except as otherwise specifically provided," conducting an "intentional[]" "intercept[]" "[of] any

wire … or electronic communication." And, because Burke knew that any communication he obtained from that intercept was the fruit of his own unlawful wiretap, he was further prohibited from "disclos[ing]" the "contents" of said communication, under § 2511(c).

Congress did not further define "intentional," but legislative history says that an "intentional" intercept is a knowing one, not inadvertent. *See* S.Rep. 99-541 at 23-24 (Congress amended the "state of mind" for the statute to "intentional" to "underscore that inadvertent interceptions are not crimes"; as emphasized in the Judiciary Committee's report, "people who steal because they like to or to get more money or to feed the poor … all commit the same crime."). The statute therefore requires at least the intent to engage in the prohibited actus reus. *See United States v. Phillips*, 19 F.3d 1565, 1576-77 (11th Cir. 1994), *amended*, 59 F.3d 1095 (11th Cir. 1995) ("[A] defendant need not intend to violate the law to commit a general intent crime but he must actually intend to do the act that the law proscribes.").

Congress did further define both "intercept" and "wire … or electronic communication." And, as Burke helpfully notes, when Congress uses "clear definitions" of terms, they are "virtually conclusive"; a court "will not deviate from an express statutory definition merely because it 'varies from the term's ordinary meaning.'" *See* Motion at 11 (quoting *Dep't of Ag. Rural Dev. Rural Housing Serv. v. Kirtz*, 601 U.S. 42, 59 (2024)).

An intentional "intercept" under the statute is the intentional "acquisition" through the use of any "electronic, mechanical, or other device." § 2510(4). An "electronic, mechanical, or other device" is "any device or apparatus which can be used to intercept" "other than" "any telephone or telegraph instrument," "equipment or facility," or "any component thereof," "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 [wire or electronic communication] service and used in the ordinary course of its business;" or one "being used by a provider … in the ordinary course of its business," (or being used by law enforcement in the ordinary course of its business or being used to correct subnormal hearing to at most normal hearing). § 2510(5)(a). A "user" is defined as a person or entity who "uses an electronic communications service; and [] is duly authorized by the provider of such service to engage in such use." § 2510(13). An "'electronic communication service' means any service which provides to users thereof the ability to send and receive wire or electronic communications." § 2510(15).

The limitation on the statutory definition of "device," to only those devices the interceptor is not using "in the ordinary course of business," under § 2510(5)(a), figures prominently in analyses of the statute. *See, e.g.*, *Watkins v.*

L.M. Berry & Co., 704 F.2d 577, 582 (11th Cir. 1983) (discussing the in-the-ordinary-course-of business exception in § 2510(5) and the "consent" exception in 2511(2)(d)); *and see Glazner v. Glazner*, 347 F.3d 1212 (11th Cir. 2003) (determining that husband's use of a device to record spouse's conversations was a violation of Title III; overruling *en banc Simpson v. Simpson*, 490 F.2d 803 (5th Cir. 1974), which had stated that husband's interspousal recording activity was conduct "in the ordinary course of business"). It neatly separates intentional from inadvertent wiretapping; if one is not tapping with a device the interceptor is intentionally using not "in the ordinary course of business," one is not tapping with a "device" at all. *See, e.g. Hall v. Earthlink Network, Inc.,* 396 F.3d 500, 503–05 (2d Cir. 2005) (ISP provider did not illegally intercept emails because internet platform/program used to intentionally acquire communication was used "in the ordinary course of business" and therefore was not a "device"). Limiting illegal wiretapping devices to devices used not "in the ordinary course of business" also neatly covers any commercial service provider's contractual arrangements with its legitimate subscribers and users. The Netflix subscriber who may be intercepting the company's communications (in the colloquial sense) to watch video streams or the Facebook or X (formerly Twitter) user who is sending and receiving direct messages to others across the platform, will not be inadvertently intercepting them via any prohibited

"device," because she will be using any acquisition device "in the ordinary course of business."

The statute does not further define "acquisition," but that term also is easily illuminated: "acquisition" is the possession of or dominion over something. *See, e.g.*, *Garcia-Bengochea v. Carnival Corp.,* 57 F.4th 916, 930 (11th Cir. 2023) ("acquire" is to "gain possession or control of; to get or obtain"); *Noel v. Hall*, 568 F.3d 743, 749 (9th Cir. 2009) (acquisition "occurs when the contents of a wire communication are captured or redirected in any way").

Regarding the communication intentionally "acquired" by a "device" not "in the ordinary course of business" (precisely, the "contents" of that communication, *see* § 2510(8), meaning other than the identity of the speakers or existence of the communication itself, *see* S.Rep. 99-541 at 13)—this Court asked the United States on May 20 (and asked its "amici"), whether the grand jury appropriately charged Burke with illegal intercept of "wire communication," "electronic communication," or both, for wiretapping video streams. Doc. 136 at 5-8; *see also* Doc. 128 at 4-5. To answer: The grand jury might properly have charged Burke with only illegal intercept of "wire" communications (because the audio/video streams were a "transfer" over an interstate facility that "contains" the human voice, regardless that it also contains other things). However, because the definition of "electronic communication" expressly excludes a wire communication, *see* § 2510(12)(A), the companion video portion of said streams, which contain no human utterances but

do include "signs, signals, writing, images, sounds, [and] data," allowed for Burke to also be charged with illegal intercept of "electronic communications." § 2510(12). As explained in the pertinent legislative history:

> It is important to recognize that a transaction may consist, in part, of both electronic communications and wire and oral communications as those terms are defined in [§ 2510 …]. Accordingly, different aspects of the same communication might be characterized differently. For example, the transmission of data over the telephone is an electronic communication. If the parties use the line to speak to one another between data transmissions, those communications would be wire communications.

See S.Rep. 99-541 at 16; *see also*, H.Rep. 99-647 at 35 (same). Thus, the audio/video streams at issue in this case are both, "wire communications" and "electronic communications." And, as previously determined by this Court, charging both raises no duplicity issues. Doc. 111 at 4-7. The unit of prosecution is the intercept.

Concerning the definition of "wire … or electronic communication," Congress originally defined a "wire communication" as "the transmission of writing, signs, signals, pictures, and sounds of all kinds by aid of wire, cable, or other like connection between the points of origin and reception of such transmission, including all instrumentalities, facilities, apparatus, and services (among other things, the receipt, forwarding, and delivery of communications) incidental to such transmission." Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064, 1065 (1934) (codified as amended at 47 U.S.C. §§ 151-154). That definition was altered in 1968 to mean:

> the transfer of a communication which includes the human voice at some point. The transfer must be made in whole or in part through the use of

> communication transmission facilities by the aid of wire, cable, or other like connection, including fiber optics. The facilities may be furnished or operated by any person engaged in providing or operating such facilities for the transmission of interstate or foreign communications or he may provide or operate those facilities for the transmission of communications affecting interstate or foreign commerce.

Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 212 (1968). In 1986, at the advent of the computer age (and immediately following the demise of "Ma Bell's" monopoly on telecommunications equipment and services, *see United States v. AT&T*, 524 F.Supp. 1336 (D.D.C. 1981); *and United States v. AT&T*, 552 F.Supp. 131 (D.D.C. 1982)), Congress redefined a "wire communication" specifically to cover the entire transmission of a telephone call, as the telecommunications industry had converted from phonelines (today, "landlines"), to other interstate communication facilities. *See* S.Rep. 99-541 at 12 ("The conversion of a voice signal to digital form for purposes of transmission does not render the communication non-wire. The term 'wire communication' includes existing telephone service, and digitized communications to the extent that they contain the human voice at the point of origin, reception, or some point in between."). A "wire communication" is now "any aural transfer"—"a transfer containing the human voice at any point between and including the point of origin and the point of reception," § 2510(18)—made via "use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception …." § 2510(1).

Also in 1986, to ensure the prohibition on illegal wiretapping kept up with remote computing and other non-telephonic communications services, *see* S.Rep. 99-541 at 3, Congress added "electronic communication" to the statute, because a statute protecting "the security and privacy of business and personal communications," was "hopelessly out of date" if it protected those interests only when a communication's "contents" could be "overheard and understood by the human ear," S.Rep. 99-541 at 2. An "electronic communication" is "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature, transmitted in whole or in part by a wire, radio electromagnetic, photoelectronic or photooptical system" that is not a "wire" communication (or that involves data transmitted through a tone-only pager or tracking device like those used by police without constitutional concern until *United States v. Jones*, 565 U.S. 400 (2012)). § 2510(12); S.Rep. 99-541 at 14.

Thus, according to its plain language, the wiretap statute prohibits the: (1) intentional; (2) acquisition; (3) by a device being used not "in the ordinary course of business"; (4) of the contents of a wire or electronic communication. *See* § 2511(1)(c). And, to answer the Court's specific statutory interpretation questions (*see* Doc. 128 at 4-5, Doc. 135 at 26-27): The Court can indeed instruct the jury under the wiretap statute using "merely" the words of the statute itself. The court should instruct the jury that it must find both intentional "acquisition" and intentional use of a device (defined in the instructions to be a

device used other than "in the ordinary course of business"), to separate lawful from unlawful conduct. *See, e.g.*, *Staples v. United States*, 511 U.S. 600 (1994). And, if instructing the jury on the affirmative defense of "consent," this Court should define the "party" who must have given prior consent as the entity at the "point of origin" of the "transfer" or "transmission" tapped or an entity at the "point of reception" of the illegally tapped transmission, who is not intentionally using a device not "in the ordinary course of business" to acquire it. § 2510(1) and (18); and see S.Rep. 99-541 at 12.

ii. Under the plain language of the statute, Congress has not threatened First Amendment injury at all.

"Because of the wide-reaching effects of striking down a statute on its face at the request of one whose own conduct may be punished despite the First Amendment," the Supreme Court has "recognized that the overbreadth doctrine is strong medicine" and "employed it with hesitation, and then only as a last resort." *See New York v. Ferber*, 458 U.S. at 769 (cleaned up). "[C]laims of facial overbreadth have been entertained in cases involving statutes which, by their terms, seek to regulate 'only spoken words.'" *Broadrick v. Oklahoma*, 413 U.S. 601, 612 (1973). The doctrine's "function, a limited one at the outset, attenuates as the otherwise unprotected behavior that it forbids the State to sanction moves from 'pure speech' toward conduct and that conduct—even if expressive—falls within the scope of

otherwise valid criminal laws." *Los Angeles Police Dep't v. United Reporting Pub. Corp.*, 528 U.S. 32, 40 (1999) (cleaned up, quoting *Broadrick*).

But here, Congress has prohibited intentional acquisition, by a device being used not "in the ordinary course of business," of something in transit over an interstate communication facility. It has not regulated spoken words, other expression, or even any speech-related conduct. The wiretap statute is essentially a theft statute, prohibiting intentionally tapping into something, without authorization, to obtain someone else's stuff. Burke therefore cannot proceed to the next step in the first task of overbreadth—determining whether the statute chills a "substantial" portion of protected speech, relative to unprotected conduct—and his overbreadth challenge fails. *Cf. United States v. Yang*, 281 F.3d 534, 544 n.2 (6th Cir. 2002) (dismissing out-of-hand defendant's challenge to the trade secrets statute under the First Amendment and stating: "We have every confidence that ordinary people seeking to steal information that they believe is a trade secret would understand that their conduct is proscribed by the statute.").

Burke, who bears the burden of establishing overbreadth in text and fact, does not actually argue to the contrary. Instead, he provides a severely truncated description of an illegal wiretap (denigrating that description as the United States' "theory," not his own): "[T]he wiretap statute prohibits the interception (acquisition of the contents)—§ 2510(4)) of any communication that contains the human voice." Doc. 125 at 1. Thus, he leaves out the requirements of "intent" to acquire by

"device" (let alone a device used not "in the ordinary course of business"). He then simply musters his parade of horribles, culminating in the wiretap statute suppressing "view[ing] and listen[ing] to each and every bit of information online." *Id*. at 4-5.

But if Burke is implying (as we think he definitely is) that "hearing" or "listening"—or downloading or streaming to hear or listen or watch—is prohibited under the plain language of the statute, he does not explain why, and the Eleventh Circuit has said otherwise. A defendant illegally intercepts a communication upon acquisition; it is not necessary for the defendant to listen to or read the communication to violate the Wiretap Act. *See United States v. Turk*, 526 F.2d 654, 658 (5th Cir. 1976) ("If a person secrets a recorder in a room and thereby records a conversation between two others, 'acquisition' occurs at the time the recording is made."); *Watkins v. L.M. Berry & Co.*, 704 F.2d at 584; *and see Sanders v. Robert Bosch Corp.*, 38 F.3d 736, 740 (4th Cir. 1994) ("recording of a telephone conversation alone constitutes an 'aural … acquisition' of that conversation"). In 1968, Congress explained that, under § 2510(4), "intercept" included "the aural acquisition of the content of any wire or oral communication" by a device but did not include "[o]ther forms of surveillance." S.Rep. 90-1097 at 62. As explained in *Turk*, that "passage indicates that the act of surveillance and ***not the literal 'aural acquisition' (i.e., the hearing)***, which might be contemporaneous with the surveillance, or might

follow therefrom, was at the center of congressional concern." *Turk*, 526 F.2d at 659 (emphasis added).

Indeed, Congress never intended to prohibit hearing or listening to anything. In 1968, in the wake of Supreme Court decisions grappling with police "eavesdropping" on telephone conversations—see, for example, *Rathbun v. United States*, 355 U.S. 107 (1957), then *Katz v. United States*, 389 U.S. 347 (1967)—Congress rewrote the "intercept" provisions of the 1934 Communications Act, drafting a statute that required law enforcement to obtain a warrant for electronic surveillance by device—and aligned private liability for the same conduct. *See*, S.Rep. 90-1097 at 2-3. Congress thus protected from intrusion by both governmental and private actors on the "privacy" interests enshrined not only in the Fourth Amendment but also in other Amendments in the Bill of Rights, including in the First's "freedom to associate and privacy in one's associations." *See Katz*, at 350 n.5.

By 1986, "Title III [was] the primary law protecting the security and privacy of business and personal communications in the United States," S.Rep. 99-541 at 2, but: "Its regimen for protecting the privacy of voice communications," designed originally to respond to developing Fourth Amendment law concerning telephone taps, *see* S.Rep. 90-1097 at 39-40, was "expressly limited to the unauthorized aural interception of wire or oral communications. It only applie[d] where the contents of a communication c[ould] be overheard and understood by the human ear." S.Rep. 99-541 at 2 (emphasis added). *And this was a problem*, because the:

> [T]remendous advances in telecommunications and computer technologies [had] carried with them comparable technological advances in surveillance devices and techniques. Electronic hardware making it possible for overzealous law enforcement agencies, industrial spies and private parties to intercept the personal or proprietary communications of others [were] readily available in the American market.

Id. at 3.

So Congress amended the statute, to enter the computer age and focus on the hardware. It eliminated the "aural" problem by redefining a wiretap as aural "or other" acquisition. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986). It added to § 2510 "electronic communication" and related provisions to cover computer technology. *See, e.g., Id*. at 1848-49. And it amended § 2510(5)(a), the "in the ordinary course of business" definition of "device," accordingly. *Id*. at 1848, 1851 (replacing "communications common carrier" with "provider of wire or electronic communication service," and inserting in § 2510(5)(a)(i), "furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business"). The wiretap statute Burke violated provides no room for overbreadth attack based on the assertion that it only "applies where the contents of a communication *can be* overheard and understood by the human ear"—and it never prohibited the overhearing and understanding itself, in the first place. That detail is completely incidental to enforcement.

Indeed, the statute under which Burke was charged cannot even be interpreted to prohibit, as an illegal wiretap, the "listening" or "viewing" anything,

for several reasons. First, the human ear or eye is not a "device." Under § 2510(5), "electronic, mechanical, or other device means any device or apparatus,"— and any "other" device therefore should be akin to a "mechanical" or "electronic" one, *see Circuit City Stores Inc. v. Adams*, 532 U.S. 105, 114-15 (2001) (applying the principle of *ejusdem generis*). And Congress *specifically exempted* from "device" a "hearing aid or similar device" that substitutes for the human ear, so long as it merely assists the wearer with hearing normally. § 2510(5)(b). Also: How would one determine whether an ear or eye is being used "in the ordinary course of business"? Physical, corporeal acquisition by ear or eye is simply not acquisition by "device" at all. *See* § 2510(5)(a).

In addition, no ear or eye "acquires" a communication as necessary to trigger the wiretap statute. Acquisition by device must occur during the "transfer" or "transmission" of a communication via interstate facility, while the digitized human voice, images, data—whatever is the wire or electronic communication—is "in flight." *See United States v. Steiger* 318 F.3d 1039, 1050 (11th Cir. 2003) (adopting this definition for an intercept of an electronic communication as well as a wire communication). The human ear or eye does not "acquire" data in this way. Finally, the ear or eye literally is useless should the wiretapper wish to acquire a "wire or electronic communication" as defined. It may be used to interpret the contents of that communication. But it cannot be said to "acquire" the communication itself.

Burke's overbreadth theory, based on his mere assertions of prohibited First Amendment activity, therefore fails under the plain language of the statute: The wiretap statute does not chill hearing or listening to (or watching) anything. *See Turk*, 526 F.2d 654. Nor does the wiretap statute regulate merely "streaming" anything—unless, of course, that "streaming" is an intentional acquisition by unauthorized device (i.e., a device not exempted under § 2510(5)).

Finally, 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. Burke continuously becomes confused on this point, because he is concentrating on his own school of red herring spawned from his "conversion" theory—that the First Amendment requires this Court to overrule *McCann* and require the United States to negate the defenses he says he will raise at trial. For instance, he states: "Only after the government shows an "unlawful" acquisition (*from a non-public server*) should the defendant be forced to prove that the acquisition was "justified" or "permitted." Doc. 125 at 18 (emphasis added). Pardon? Burke's charged acquisitions were not unlawful because he intended to access a "non-public server"; Burke's acquisitions, as charged, were unlawful because he knew he was acquiring, and intended to acquire, multiple communications using a device not "in the ordinary course of business." And his further use or disclosure of the contents of those communications is unlawful

because he knew the communications had been unlawfully obtained (because he had unlawfully obtained them). The innocent consumer of Internet content, on whose behalf Burke challenges the wiretap statute, is indeed innocent, because that consumer bears no unlawful intent under the wiretap statute.

And yet again, Burke offers no authority suggesting that the wiretap's prohibition on device intercept prohibits something protected by the First Amendment; the closest he comes is a quotation from *Stanley v. Georgia*, 394 U.S. 557, 564 (1969): "[T]he Constitution protects the right to receive information and ideas … regardless of their social worth." Of course it does. But it does so by protecting the right to speak and publish, and "[t]he right to speak and publish does not carry with it the unrestrained right to gather information." *Zemel v. Rusk*, 381 U.S. 1, 17 (1965).

Indeed, the First Amendment protects "receipt" of information because: "It is the purpose of the First Amendment to preserve an uninhibited marketplace of ideas in which truth will ultimately prevail . . .. It is the right of the public to receive suitable access to social, political, esthetic, moral, and other ideas and experiences which is crucial." *Red Lion Broadcasting Co. v. FCC*, 395 U.S. 367, 390. There is no recognized "right to listen" under the First Amendment—and the Supreme Court recently said as much, in *Murthy v. Missouri*, 603 U.S. 43 (2024). There, the Court summarily rejected (when assessing the fundamental constitutional concept of judicial authority over "case and controversy") the theory that one suffers First

Amendment injury by infringement on one's "right to listen" to anyone speaking over a social media platform, stating: "While we have recognized a 'First Amendment right to 'receive information and ideas,' we have identified a cognizable injury only where the listener has a concrete, specific connection to the speaker." *Id.* at 75 (cleaned up). And here, any defendant intentionally intercepting by device not "in the ordinary course of business" has no "connection" to the "speaker" of the "received information and ideas" at all; he is intentionally *taking*, with a device he is using not "in the ordinary course of business," a private and protected "communication." It is difficult to see, therefore, how Burke can assert First Amendment injury on any defendant's behalf at all, in order to trigger the narrow exception for overbreadth challenge to the otherwise broad prohibition on facial challenge to a statute.

The Constitution does not provide Burke the right to *take* others' private and proprietary information, by intentionally tapping into their communications via unauthorized device. As explained in *Branzburg v. Hayes*, 408 U.S. 665, 691–92 (1972): "Although stealing documents or private wiretapping could provide newsworthy information, neither reporter nor source is immune from conviction for such conduct, whatever the impact on the flow of news. … The Amendment does not reach so far as to override the interest of the public in ensuring that neither reporter nor source is invading the rights of other citizens through reprehensible conduct forbidden to all other persons." Congress may prohibit the theft of a book,

without running afoul of the First Amendment, regardless that the book contains speech that the author has the right to write, the publisher to publish, and the reader to read. The wiretap statute protects against both governmental and non-governmental invasion of our privacy rights—and our freedom from equivalent private conduct. It certainly may prohibit Burke's intentional acquisition by unauthorized device of wire or electronic communications in transit over an interstate wire facility, without impaling the statute on the First Amendment.

Indeed, illegal wiretapping—and, in very particular, Burke's charged wiretaps—is the threat to First Amendment protected freedoms here. If our private communications are available for the taking, we are certainly deterred from speaking. If a communication or ***content*** provider's proprietary material is easily vulnerable to theft, it is deterred from developing its business. If a media outlet's private deliberations regarding the publishing of news are hack-able, how can that not affect freedom of the press and all our dependent freedoms.

As this Court observed in its previous Order (Doc. 110 at 10): When a defendant procures the used or disclosed contents of a communication himself, "a prohibition on the publication of [those communications] operates as an effective deterrent against the initial unlawful acquisition of that same information." *Dahlstrom v. Sun-Times Media, LLC* , 777 F.3d 937, 952 (7th Cir. 2015). And rendering unlawful that initial acquisition of the communication containing the then-reviewed-and-disclosed information protects not only constitutional "privacy"

(and other) interests enshrined in the Fourth Amendment but the "privacy in one's associations" enshrined in the First, *see Katz v. United States*, 389 U.S. 347, 350 & n.5, as well.

An illegal wiretapper, not Congress, chills our First Amendment-recognized freedoms.

iii. Burke fails to explain why, if the statute prohibits protected speech in any way, it prohibits a "substantial amount" of such speech in relation to unprotected speech or other conduct.

Even if Burke could explain how the wiretap statute burdens freedom of speech, he has no argument whatsoever for why it burdens the "substantial amount" of protected speech—either "in an absolute sense" or "relative to the statute's plainly legitimate sweep," *Williams*, 553 U.S. at 292 (emphasis omitted)—necessary to apply the "strong medicine" of overbreadth remedy.

Any intrusion on First Amendment freedoms engendered by a prohibition on intentionally acquiring others' communications, by using an acquisition device in a manner not "in the ordinary course of business," is certainly incidental; indeed, infinitesimal. Any regulation of speech as such is limited to a restriction on the use of a "particularly intolerable (and socially unnecessary) mode," not even of providing, but receiving, Burke says, of whatever then-unknown "idea the speaker wishes to convey," *see R.A.V. v. City of St. Paul*, 505 U.S. 377, 393 (1992).

The wiretap statute is not Congressional First Amendment overreach.

B. Burke's overbreadth "conversion" theory—that, if the Court revisits its interpretation of the statute under *McCann* and decides that his affirmative defenses are actually elements, the wiretap statute will be less overbroad—makes no sense.

This Court also asked whether, if Burke did establish that § 2511(1) prohibits watching a video on an Internet streaming platform or visiting a public-facing webpage (which he did not), converting the statutory exceptions Burke purportedly wishes to raise at trial as affirmative defenses—"prior" "party" "consent" to his wiretap by device, under § 2511(2)(d) (no harm, so no foul of the privacy interests of the parties at either end of the transmission); or that the system he wiretapped was "configured so that" the communications he acquired by using a device outside its intended purpose were already "readily accessible to the public," under § 2511(2)(g) (no harm, so no foul of the system provider's privacy interests)—to elements, will solve the purported overbreadth problem. Again, Burke's lack of overbreadth analysis is glaring—and debilitating. Proper overbreadth analysis, at least of a "bare" overbreadth challenge like Burke's (starting without a clear prohibition on speech, so that the reviewer cannot weigh the statute's effect on protected speech versus unprotected speech), should be of both initial prohibition and exceptions to liability. But in any event, Burke also does not explain how the statutory exceptions under § 2511(2)—even the two exceptions he says he will raise at trial—affect the overbreadth analysis in the first place.

Nowhere in his Motion does Burke articulate the overbreadth presumption at the heart of his conversion theory: That, when reviewing for First Amendment overbreadth, this Court must review a statute's prohibitions while blinding itself to statutory exceptions to liability. And that assertion makes no constitutional sense. Overbreadth is from the point of view of the person against whom a statute will be enforced. Separating Congressional exceptions into elements or affirmative defenses is a task to ensure Due Process at trial; the defendant will be tasked at trial with raising a statutory exception as an "affirmative defense" precisely when he, not the government, is in the best position to know whether the exception applies. It therefore is illogical that the "chilling" effect on a potential defendant under overbreadth analysis would include only "elements" of the crime (determined for purposes of the Fifth Amendment right to indictment by grand jury and the Sixth Amendment right to trial by petit jury), but not those "affirmative defenses" that are often within the defendant's peculiar ken.

In *Ashcroft v. Free Speech Coal.*, 535 U.S. 234, 256 (2002), the Supreme Court decided that, "[e]ven if an affirmative defense can save a statute from First Amendment challenge," there the "defense [was] incomplete and insufficient, even on its own terms." But the Court was assessing a statutory exception it already had decided posed serious "ken" problems for the defendant—and, in any event, the Court's musing on whether overbreadth includes assessment of statutory exceptions was clearly dicta. In *Ashcroft v. ACLU*, 542 U.S. 656, 670-71 (2004), (assessing the

same statute), the Supreme Court again expressed skepticism regarding an overbreadth analysis that includes statutory exceptions, stating: "Where a prosecution is a likely possibility, yet only an affirmative defense is available, speakers may self-censor rather than risk the perils of trial. There is a potential for extraordinary harm and a serious chill upon protected speech." But again, this was pure dicta, and it was uttered after finding a "likely possibility" of prosecution—which Burke certainly has not shown here.

Moreover, and very importantly: In both *Ashcroft*s, the defendant challenging his criminal conviction by asserting others' First Amendment rights already had carried his burden, in "text and fact," to show *potential* overbreadth by establishing that the statute in question actually entrenched on speech. Indeed, in both cases, the overbreadth challenge was a traditional overbreadth complaint, arguing that, because the statute clearly targeted speech (images of sexual abuse of children, or "child pornography"), the question was whether it prohibited enough speech—and enough protected speech, as opposed to unprotected speech—that the benefits of statute outweigh its First Amendment cost. *See United States v. Williams*, 553 U.S. at 292–93 ("In order to maintain an appropriate balance" of "societal costs," "we have vigorously enforced the requirement that a statute's overbreadth be substantial, not only in an absolute sense, but also relative to the statute's plainly legitimate sweep." (emphasis in original)). Here, in contrast, Burke brings a "bare" overbreadth challenge to the statute, asking this Court itself to find some speech regulated, and

proceed from there. Indeed, it is unclear, in light of pronouncements like that in *Williams*, that such a challenge ever can succeed. But regardless, Burke has never established, in text or fact, even the possibility of overbreadth. He should not be able to take advantage of any benefit of the doubt that might be afforded under the *Ashcroft*s' dicta.

In any event, Burke fails, yet again, to explain his legal premise: That converting the affirmative defenses he wishes to raise into elements reduces the wiretap statute's First Amendment footprint. Indeed, if the wiretap statute, by prohibiting the intentional acquisition by unauthorized device of a communication, could be said to restrict the "unconsented to" receipt of expressive speech (and the exceptions to alleviate that restriction), that restriction would clearly be incidental to Congress's primary goal of protecting the speaker's own privacy and proprietary interests in their speech. The appropriate First Amendment challenge would be not an overbreadth challenge but a "direct" First Amendment challenge, asserting that those incidental restrictions are greater than necessary to further those interests. *See San Francisco Arts & Athletics, Inc. v. U.S. Olympic Comm.*, 483 U.S. 522, 536–37 (1987). Interpreting the statute to require the government to prove lack of consent in the first place would not affect the scope of speech restricted, at all.

The United States is unable even to create a straw man for Burke here; he needs to carry his own overbreadth burdens. His "conversion theory" fails.

C. This Court therefore need not revisit its decision that *McCann* defeats Burke's Fifth and Sixth Amendment challenges to his indictment based on Congress's allocation of the burden of proof to him for his preferred defenses.

Burke, therefore, has no viable overbreadth challenge. He has not even attempted to carry his burden of showing, in law and fact, that the wiretap statute prohibits speech, or that it chills an impermissibly large swath of protected speech while legitimately prohibiting unprotected speech.

Should this Court determine otherwise, however, and decide to apply the "strong medicine" of overbreadth to render the wiretap statute unconstitutional (unless the United States proves beyond a reasonable doubt at trial the lack of prior consent to the prohibited wiretapping conduct), the remedy is not to interpret *McCann* differently in order to avoid damaging the statute itself. That the Eleventh Circuit created support for Burke's "conversion" theory, by determining that Congress's exceptions to wiretap liability are affirmative defenses, is—if true—simply a legal fact. The United States knows of no doctrine the District Court may employ to avoid the situation: *McCann* clearly does *not* speak to the "consequent" issue of First Amendment overbreadth, and this Court therefore cannot evaluate that "implicit holding" in light of later statutory amendments. The *McCann* Court, if presented with that secondary issue, *might* have been able, under principles of "constitutional avoidance," to interpret the statute differently. But it obviously was not presented with that issue, and its resolution of the Fifth and Sixth Amendment

"affirmative defense versus element" issue in no way depends on a prior determination of any First Amendment issue. It is therefore now for the Eleventh Circuit, in a subsequent case, to grapple with this problem, if it exists at all (it does not).

Should this Court determine that the wiretap statute is fatally overbroad, it should dismiss the grand jury's wiretap charges, allowing the United States to appeal immediately or to seek a superseding indictment charging (and requiring proof at trial beyond a reasonable doubt) the absence of Burke's preferred affirmative defenses. If the United States chooses the latter, Burke at that time can challenge the new indictment as still unconstitutional (and, we are sure, he will). He can then explain why that remedy is not sufficient to protect others from Congress's First Amendment overreach.

IV. Conclusion

This Court should deny Burke's Third Motion to Dismiss.

Respectfully submitted,

GREGORY W. KEHOE
United States Attorney

By: */s/Jay G. Trezevant*
Jay G. Trezevant
Assistant United States Attorney
Florida Bar No. 0802093
400 N. Tampa Street, Suite 3200
Tampa, Florida 33602-4798
Telephone: (813) 274-6000
Facsimile: (813) 274-6358
E-mail: jay.trezevant@usdoj.gov

/s/ Adam J. Duso

Adam J. Duso
Assistant United States Attorney
Florida Bar No. 1026003
400 N. Tampa St., Suite 3200
Tampa, Florida 33602-4798
Telephone: (813) 274-6000
Email: adam.duso@usdoj.gov

U.S. v. Timothy Burke **Case No. 8:24-cr-68-KKM-TGW**

CERTIFICATE OF SERVICE

I hereby certify that on June 23, 2025, I electronically filed the foregoing with the Clerk of the Court by using the CM/ECF system which will send a notice of electronic filing to the following:

Michael Maddux, Esq.
Mark Rasch, Esq.

/s/ Jay G. Trezevant
Jay G. Trezevant
Assistant United States Attorney