UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

UNITED STATES OF AMERICA,

v. Case No.: 8:24-cr-00068-KKM-TGW

TIMOTHY BURKE,

Defendant.

AMICUS BRIEF OF ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS

Alan Butler
Counsel of Record
Electronic Privacy Information Center (EPIC)
1519 New Hampshire Ave NW,
Washington, D.C., 20036
(202) 483–1140
butler@epic.org

Counsel for Amicus Curiae

TABLE OF AUTHORITIES

CASES

STATUTES

LEGISLATIVE MATERIALS

INTEREST OF *AMICUS CURIAE*

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC regularly participates as amicus in cases concerning the scope and application of federal privacy statutes. *See, e.g.*, *Vita v. New England Baptist*, 243 N.E. 3d 1185 (Mass. 2024); *Facebook, Inc. v. State*, 296 A.3d 492 (N.J. 2023).

SUMMARY OF THE ARGUMENT

Congress passed the Wiretap Act in 1968 to ensure that telephone calls and other oral and wire communications would be sufficiently protected from interception by third party entities, whether government or non-government. The law was significantly amended two decades later in light of the technological evolutions that brought communications into the digital era. But much has changed since Congress passed the Electronic Communications Privacy Act in 1986, and the statute can be challenging to interpret in some modern contexts. Nevertheless, the law provides important safeguards against unchecked government and corporate surveillance.

This case presents important and novel questions of statutory interpretation and policy related to the privacy protections in the Wiretap Act. While this case involves a criminal indictment, the Court's interpretation of the statute has far-reaching implications because of the broad civil and criminal penalties applicable to violations of the Act. The Court has invited amicus curiae to submit briefing on three specific issues (Order at 4-5, Dkt 128) related to the definitions in Section 2510 and the scope of the prohibitions in Section 2511(1). This brief addresses those three questions, albeit slightly out of order. This brief necessarily begins with the Court's second question, because it should be dispositive for the Wiretap Act claims at issue here. Defendant Burke was a party to the communication between

the video streaming server and his device(s), and thus, the Government has not stated a claim under Section 2511(1)(a). In the streaming context, the operative communication is the transfer of video data from the streaming server to the recipient user's device. As a direct party to that communication, the user cannot be held liable for third-party interception when communicating with a streaming server, regardless of what data is included in the stream.

To the Court's first question, the transmission of video data, which includes human voice data, from a streaming server to a recipient's computer is best interpreted as an electronic communication, though this distinction is likely not dispositive. An "electronic communication" broadly includes the "transfer of . . . signals . . . images, sounds, [and] data . . ." 18 U.S.C. § 2510(12). The one-way transmission of mixed video and audio data in a video stream is distinguishable from a direct communication (1-to-1 or more), such as a video call, which involves real time communication between people on both ends and would be best categorized as a wire communication.

To the Court's third and final question, it is not necessary to adopt any special pleading requirement regarding the "readily accessible" exception, but the Court should be mindful of the First Amendment implications of Wiretap Act liability that would limit journalistic reporting on matters of public concern as discussed in *Bartnicki v. Vopper,* 532 U.S. 514 (2001). There would

be significant First Amendment concerns to everyday, basic internet use if the Court does not read third party interception as a baseline element of an 2511(1)(a) offense.

ARGUMENT

The unlawful interception charges in this case should be dismissed because the allegations do not state a claim of third-party interception of a wire or electronic communication. The Court has invited amicus curiae to submit briefing on three specific issues (Order at 4-5, Dkt 128) related to the definitions in Section 2510 and the scope of the prohibitions in Section 2511(1).

The Government in this case alleges that Defendant Burke violated the Wiretap Act, 18 U.S.C. § 2511(1)(a), when he accessed and downloaded video content "being streamed across the StreamCo-Net for quality assurance and other business-related purposes." (Indictment at 4, ¶ 9). This stream included live video and audio of interviews as well as pre- and post-production conversations recorded by a multinational news network. (*Id.* at 15-16, ¶ 23(i)). Defendant Burke argues, among other things, that the Government has failed to state a claim under the Wiretap Act (Third Mot. to Dismiss at 1, Dkt 125). EPIC submits this brief as an *amicus curiae* in support of Defendant Burke's motion because the Wiretap Act does not prohibit individuals from accessing video or audio streams as an internet user, and any interpretation to the contrary would present First Amendment overbreadth concerns and undermine the statutory scheme.

One preliminary point that is relevant to all three of the Court's questions of interpretation is that the scope of the Wiretap Act is best understood relative to its temporal nature. As Professor Andrew Serwin explains, the Act "only applies to conduct that occurs at the precise time of transmission." 1 Serwin, *Information Security and Privacy: A Guide to Federal and State Law and Compliance*, §7:5, at 391 (2015). This temporal component is what distinguishes the Wiretap Act from its sister statute, the Stored Communications Act. *Id.*[1] And it is relevant here because it helps to focus the analysis on the precise communication at issue, namely, the transfer between the StreamCo-Net server and the recipient devices identified in the indictment.

To begin with the Court's Second question, the short answer is: no, Section 2511(1)(a) does not prohibit a person from watching a video on an internet streaming platform or visiting a public-facing webpage. That result is, and should be, quite intuitive (even if the statutory definitions obscure it somewhat). The "communication" at issue in this case, and the operative communication channel in any video streaming service, is the transfer of data from a streaming server to the recipient user's computer. As a "direct party"

[1] *See also* Bruce E. Boyden, *Can a Computer Intercept Your Email?*, 34 Cardozo L. Rev. 669, 680 (2012).

to this communication, the Defendant cannot be held liable for third party interception. 18 U.S.C. § 2511(2)(d); *see United States v. Szymuszkiewicz*, 622 F3d. 701, 707 (7th Cir. 2010). The third party interception requirement, described by the Seventh Circuit in *Szymuszkiewicz* and in other cases cited therein, is best understood as an inherent element of the crime of unlawful interception under the Wiretap Act, rather than as an "exception" to that offense. *See* 622 F3d. at 707.

The Government confuses this issue substantially in the presentation of its indictment and its briefing on the Defendant's motion to dismiss. The Wiretap Act is, at bottom, a statute that prohibits an individual from using "a machine to capture the communications *of others*." Charles Doyle, *Privacy: An Abridged Overview of the Electronic Communications Privacy Act*, CRS R41734 (Oct. 9, 2012). The Government focuses at length in its opposition on the "device" definition in Section 2510(5). (Gov't Opp., Dkt 138, at 17–20). But as Judge Easterbrook explains in the Seventh Circuit's decision in *Szymuszkiewicz*, 622 F.3d at 707, the device requirement is typically not relevant (and is usually trivially satisfied) when there is a third party interception of electronic communications. The phrase "ordinary course of business" is used to define a narrow carve out from the device definition to ensure that routine routing and transiting of communications does not create wiretap liability for service providers or other related entities. Nothing in

that definition undercuts the core premise and focus of the Wiretap Act, which is on interception by third parties to a communication.

Not only is the device definition irrelevant in this case, but the Government's proposed reliance on the "ordinary course of business" terminology to determine whether an internet user's conduct violates federal law would be an unprecedented and unpredictable departure from existing doctrine. The question of whether a particular use of a device, whether it is a computer or accessory or otherwise, is within the scope of ordinary use would devolve into interminable factual disputes in every case. And untethered from the third-party interception requirement, it could call into question the legality of any number of devices used to access, play, or modify video and audio content on the internet.

The Court's other two questions require a slightly longer analysis but support this same ultimate conclusion. The short answer to the Court's first question (Order, Dkt 128 at 4) is that neither the statute nor prior cases directly answer the classification question of whether streaming video that includes the human voice combined with visual data is an electronic communication, or a wire communication, or both. But we believe that the statute is best read to treat such streaming transfers as electronic communications, as distinguished from point-to-point voice communications similar to a telephone call. The answer to this question is likely not

dispositive to the case given that the Defendant was a direct party to the communication, but it would be relevant if the Court intends to reach the "readily accessible to the general public" exclusion under Section 2511(2)(g).

Mixed video-audio recordings that are transferred over the Internet could arguably meet either the definition of an electronic communication under Section 2510(10) or the definition of a wire communication under Section 2510(1). To our knowledge, no court has answered this question directly. Both the context of the statute's history and the broader technological context of modern internet systems suggests that video streaming communications should be treated as electronic communications for the purposes of the Wiretap Act.

The Wiretap Act was created by Section 802 of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, 82 Stat. 212 (1968). At that time, the law was focused on "safeguard[ing] the privacy of innocent persons" from both government and private interception. Section 801, 82 Stat. at 211. The statute as originally enacted to protect wire communications and oral communications. Congress later amended the law in 1986 when it passed the Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1848 (1986). Those amendments extended statutory protections to electronic communications in recognition of the rapid expansion of digital networks, and Congress gave the new category a "broad,

functional" definition. *In re Pharmatrak, Inc.*, 329 F.3d 9, 18 (1st Cir. 2003) (quoting *Brown v. Waddell*, 50 F.3d 285, 289 (4th Cir. 1995)).

There is no question that the streaming transfers at issue in this case fit within the broad definition of an "electronic communication" because they involved the "transfer of . . . signals . . . images, sounds, [and] data . . . ." 18 U.S.C. § 2510(12). But Congress specifically excluded four categories of communications from that definition, including "any wire or oral communication." 18 U.S.C. § 2510(12)(A). On its face, the statute seems to say that streaming transfers cannot be both an electronic communication and a wire communication because those are defined as separate categories. However, the Senate in its Judiciary Committee report on ECPA stated that:

> It is important to recognize that a transaction may consist, in part, of both electronic communications and wire or oral communications as those terms are defined. . . . 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.

S. Rep. No. 99-541, at 16 (Oct. 21, 1986). Congress appears, by this report, to have contemplated that some file transfers that contain both human voice data and other data could be characterized as part wire communication and part electronic communication. But it is not clear how such mixed communications are to be treated in those few instances where the rules for wire and electronic communications differ.

This case presents a novel question that does not appear to have been addressed by previous courts or by Congress: what is the proper classification under Section 2510 of a digital transfer (or stream) of a file that includes human voices in its mixed video and audio data? In the case of a streaming service, the video and audio data are being presented to the recipient in real time from either a live or prerecorded source. But this example is further distinguishable from a "video call" that involves a direct communication (1-to-1) in real time between people on both ends,[2] and from a conference call or other multi-party communication equivalent to a telephone communication.

We believe that online file transfers and mixed video/audio streams should fit within the electronic communications definition even if their audio data includes human voice recordings. Congress narrowed the scope of the wire communication definition when it amended the statute in ECPA and courts have not treated other similar audiovisual transfers (such as cable and satellite broadcasts) as wire communications. Specifically, the ECPA amendments modified the wire communication definition in Section 2510(1) by replacing the phrase "any communication" with "any aural transfer" and

[2] One court has reasoned that video calls made by inmates in a detention facility are wire communications, even though "the audio and video data usually traveled 'through two separate data streams,'" because they "originated together at the video tablet . . . and then were 'assembled by the receiving device.'" *United States v. Serna*, No. 22-cr-1194, 2024 WL 1902759 at *6 (S.D. Tex. Jan. 31, 2024). The court found that this meant 'the video data were part of a transfer containing the human voice at "the point of origin and the point of reception."' *Id.*

adding the phrase "or other" after aural in the interception definition in Section 2510(4). The amendments also added a definition of aural transfer: "a transfer containing the human voice at any point between and including the point of origin and the point of reception." 18 U.S.C. § 2510(18).

The intent of Congress in the ECPA amendments was to broaden the scope of protected communication to preserve privacy in the face of rapid technological evolution. But Congress recognized that it should be careful not to inadvertently impose liability on radio hobbyists (for example) and others who might inadvertently intercept broadcast communications. This intent is effectuated in part through the "readily available to the general public" exception. Indeed, Congress went so far in creating the broad "readily available" carve out, and the "cordless phone" exclusion from the wire and electronic communications definitions, that it had to amend the statute again in the Communications Assistance for Law Enforcement Act of 1994, Pub. L. 103-414, 108 Stat. 4279, to ensure that private communications were sufficiently protected.

The 1994 amendments were informed by a 1991 report of the Privacy and Technology Task Force, created by Senator Patrick Leahy and chaired by John Podesta, which recommended that Congress consider "eliminat[ing] the exemption for cordless phones, while preserving an exception for unintentional or accidental private party interception." Final Report of the

Privacy and Technology Task Force Submitted to Senator Patrick Leahy (May 29, 1991), *reprinted in* S. Hrg. 103-1022 (Mar. 18 & Aug. 11, 1994), at 183. The Task Force reviewed the Wiretap Act provisions and ECPA amendments and considered the impact of new technologies including cordless and mobile phones, electronic mail, and out-of-band signaling in advanced telephone communications. *Id.* The Task Force Report distinguishes between "voice and nonvoice electronic communications" and refers to wire communications with the shorthand of "(voice)" and emphasizes the distinction between the protections of Title I of ECPA (Sections 2511 et seq.), which protects such communications while "in transit," with Title II of ECPA (Sections 2701 et seq.), which protect data in electronic storage. *Id.* at 180.

Even after the 1994 amendments, the statute remains ambiguous about the precise interaction between the wire communication and electronic communication definitions in Section 2510 with the readily accessible exception in Section 2511(2)(g). Notably, the Task Force Report did not mention cable or satellite communications at all in its analysis, even though those signals contain human voice audio data. And the Task Force discussed at length the reasoning behind the carve out for cordless phones and whether various forms of radio communications (including human voice data) would be considered "readily accessible to the general public." *Id.* at 181–84. So

there was certainly not consensus, nor even a sense, at the time the 1994 amendments were being considered that digital broadcast transfers of mixed audio and video data would be subject to different rules than other digital broadcast transfers. Indeed, such a cramped interpretation of Sections 2510 and 2511 would have caused major problems with both the civil and criminal applications of the Wiretap Act. This is especially true because the exclusion of wire communications from the "readily accessible" exemption would defeat one of the primary purposes of that exemption, to protect radio hobbyists from liability for accessing other radio signals, if broadcast messages involving the human voice were considered wire communications not subject to the exemption.

The Court's final question concerns the potential First Amendment implications of allowing the Government to broadly construe the statute in an indictment and shift the burden on to a defendant to prove certain elements. In general, the Court has identified the appropriate framework for evaluating the First Amendment implications of the unlawful interception and use restrictions in the framework established by the Supreme Court in *Bartnicki v. Vopper*, 532 U.S. 514 (2001). But there would be additional overbreadth and chilling effects concerns if the Court does not read third-party interception as an element of the offense of interception under 2511(1)(a). This is for the simple reason that most of the routine functioning of internet

systems involves the "acquisition" of the contents of electronic communications. And for internet users, every act of browsing, streaming, visiting, or interacting with apps and websites involves a form of acquisition *as a party to the communication* between their device and a web server.

Indeed, the Government's repeated focus in its Opposition on the "proprietary" nature of the audio/video streams in this case reveals why the charges are so untethered from the purpose of the Wiretap Act, which is to protect the *privacy* of communications. When Alice calls Bob or sends an e-mail to Bob, she assumes that message will remain private and will not be intercepted by Eve. But when Bob and Alice record a podcast and post the feed of that recording on a publicly accessible link they are intending to communicate it in a stream to Carol or Dave or Frank or any other of the hundreds (or thousands) of users who may choose to access the stream. That type of streaming access simply does not implicate Section 2511(1)(a) of the Wiretap Act.

CONCLUSION

For the foregoing reasons the Court should grant the Defendant's Motion to Dismiss.

Dated: June 26, 2025

Respectfully submitted,

/s/ Alan Butler

Alan Butler
Counsel of Record

Maria Villegas Bravo
EPIC Law Fellow

Electronic Privacy Information Center (EPIC)
1519 New Hampshire Ave NW,
Washington, D.C., 20036
(202) 483–1140
butler@epic.org