UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF FLORIDA
TAMPA DIVISION

UNITED STATES OF AMERICA, **Plaintiff,** **v.** **TIMOTHY BURKE** **Defendant.**	**Case No.: 8:24-CR-68-KKM-TGW**

Brief of American Civil Liberties Union, American Civil Liberties Union of Florida, Electronic Frontier Foundation, Florida First Amendment Foundation, Free Press, Freedom of the Press Foundation, and Professor Jane Bambauer as *Amici Curiae* in Support of Defendant, and in Response to Questions (2) and (3) from the ORDER on May 21, 2025

INTRODUCTION

When a person enters a URL into their browser and watches a livestream, have they committed a prima facie violation of the Wiretap Act? How about a hobbyist who tunes into a rarely-used CB radio channel? Or anyone who listens to a live broadcast on their FM radio?

The Wiretap Act ("the Act") punishes any person who "intentionally intercepts . . . any . . . electronic communication." 18 U.S.C. § 2511(1). The definition of "electronic communication" covers "any transfer of signs, signals, writing, images," and other data transmitted electronically. *Id.* § 2510(12). The definition makes no reference to consent or expectations of privacy. *Id.* The Act's prohibition on interception includes several exceptions, including where

the person is "a party to the communication," a party "has given prior consent," or where the "electronic communication is readily accessible to the general public." *Id.* § 2511(2)(d), (2)(g)(i).

Defendant Burke was indicted under this statute. He has argued that his indictment was defective because it fails to include those statutory exceptions. *See* Mot. to Dismiss at 8–13 (Doc. 64). This Court concluded that those exceptions were affirmative defenses instead of required elements. *See* 4/14/2025 Order at 14–15 (Doc. 110). Burke filed another motion to dismiss, in part arguing that the Court's reading violates the First Amendment. Third Mot. to Dismiss at 5–10 (Doc. 125). This Court invited amici to provide guidance on this issue, and others. 5/21/2025 Order at 4–5 (Doc. 128).

In this brief, amici answer the Court's second and third questions: whether Section 2511(1)(a)'s prohibition on intercepting electronic communications reaches "watching a video on an internet streaming platform or visiting a public-facing webpage," whether doing so would nevertheless "be deemed lawful by an exception in 18 U.S.C. § 2511," and whether the First Amendment requires the government to prove that those exceptions do not apply when prosecuting a purported violation. *Id.*

The text of Section 2511(1)(a) plainly captures such conduct, and it would fall under the Act's exceptions. But finding those exceptions to be

affirmative defenses would distort the statute's purpose and create intractable outcomes—and it would also run up against the First Amendment.

The solution is to require the Act's exceptions to be negated as elements. The alternative would only shield a person engaged in noncriminal, everyday activities from prosecution by dint of an affirmative defense, which would run counter to the purpose and text of the Wiretap Act, and would violate the First Amendment. Because the Wiretap Act is part of a communications *privacy* statute, a complaint under the Act must establish that the communications the defendant accessed were meaningfully private. And, because requiring a defendant to instead prove the exceptions as affirmative defenses would impermissibly burden the First Amendment right of listeners, information gatherers, and speakers, including journalists, Sections 2511(2)(d) and (2)(g)(i) must be read as elements of the offense to avoid serious constitutional questions. The rule of lenity requires the same.

Sections 2511(2)(d) and (2)(g)(i) make clear that the receipt of communications by intended parties or by the recipients of publicly-available content is not unlawful. But these "interceptions" are so common, expected, and often *desired* that they must operate as meaningful restrictions on the scope of the main prohibition. Prosecutors and civil plaintiffs must negate them in their pleadings.

INTERESTS OF AMICI CURIAE[1]

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit organization that since 1920 has sought to protect the civil liberties of all Americans. The American Civil Liberties Union of Florida is a state affiliate of the ACLU. The ACLU and its affiliates have appeared as both counsel and amici in numerous free speech and free press cases.

The Electronic Frontier Foundation ("EFF") is a nonprofit civil liberties organization with more than 30,000 active donors that has worked since 1990 to ensure that technology supports freedom, justice, and innovation for all people. EFF is dedicated to protecting online users' free expression and privacy rights and has fought for both in courts and legislatures across the country.

The First Amendment Foundation is a nonpartisan, nonprofit organization, based in Florida and dedicated to safeguarding and promoting the fundamental freedoms of expression recognized in the First Amendment.

Free Press is a nonpartisan, nonprofit, nationwide media and technology advocacy organization. Free Press engages in litigation, congressional advocacy, and administrative agency proceedings to safeguard the freedom of expression and freedom of the press.

[1] Counsel for amici curiae certifies that no counsel for a party authored this brief in whole or in part, and no person other than amici curiae, their members, or their counsel made a monetary contribution to the brief's preparation or submission.

Freedom of the Press Foundation ("FPF") is a nonprofit organization dedicated to defending and protecting public interest journalism. In addition to advocating for journalists' rights and freedoms, FPF documents press freedom violations around the country, develops software tools that help journalists communicate with sources confidentially, and provides digital security training to newsrooms.

Professor Jane Bambauer is the Brechner Eminent Scholar Chair at the College of Journalism and Communications and the Levin College of Law at the University of Florida. She teaches First Amendment, AI and the Law, Tort Law, and Privacy Law, and serves on the National AI Advisory Committee Subcommittee on Law Enforcement. Her work analyzes how regulation of new information technologies affects free speech, privacy, law enforcement, health and safety, competitive markets, and government accountability.

ARGUMENT

I. As a Matter of Statutory Construction, Sections 2511(2)(d) and (2)(g)(i) Must Be Read as Elements of the Offense.

Without its exceptions, the Wiretap Act would prohibit even "watching a video on an internet streaming platform or visiting a public-facing webpage." 5/21/2025 Order at 4 (Doc. 128). Sections 2511(2)(d) and (2)(g)(i), exceptions where there is "consent" or where the communication is "readily accessible," respectively, prevent the statute from reaching too far into quotidian, legal

conduct. Reading them as affirmative defenses cannot be squared with the Act's purpose and the absurdity doctrine.

A. The Act's definition of "intercept" captures a wide range of conduct that does not violate the statute via its exceptions.

Although the term "intercept" has a connotation of mischief in ordinary usage, the statutory definition is surprisingly capacious: the "acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device." 18 U.S.C. § 2510(4). This, on its face, includes watching a video online—acquiring the contents of an electronic communication through an electronic device—and visiting a public-facing webpage, which falls within that same definition.

It may be tempting to read into this definition the unstated limitation that an intended recipient of a message does not "intercept" their own communication. But the statute instead gives recipients a specific exception. *See id.* § 2511(2)(d) (exception for parties to the communication). Similarly, the exclusion of communications that are "readily accessible to the general public" appears only in the Act's exceptions. *Id.* § 2511(2)(g)(i).

Notably, in contrast to the definition of "intercept," the Act's *prohibition* on interceptions expressly excludes the exceptions "otherwise specifically

provided in this chapter." *Id.* § 2511(1). Indeed, it opens with that language. *Id.* ("Except as otherwise specifically provided . . .").[2]

B. The Act's exceptions cannot be affirmative defenses because it cannot define a cogent offense without them.

This Court has acknowledged that *United States v. McArthur*, 108 F.3d 1350 (11th Cir. 1997), sets the standard for distinguishing prima facie elements from affirmative defenses. 4/14/2025 Order at 15 (Doc. 110). "[W]here one can omit the exception from the statute without doing violence to the definition of the offense, the exception is more likely an affirmative defense." *McArthur*, 108 F.3d at 1353.

This Court found that "§ 2511(1)(a) 'defines a perfectly cogent offense' without looking to the host of statutory exceptions located in other subsections." 4/14/2025 Order at 21 (Doc. 110). We respectfully disagree. Given

---

[2] The government's new argument that the business extension exception adequately shields perfectly legal conduct from liability, *see* Opp. to Mot. to Dismiss at 7–8 (Doc. 138), is unavailing. First, it makes no structural sense that Congress would have excluded commonplace conduct that could plausibly trigger liability through an exception within a definition, 18 U.S.C. § 2510(5)(a), rather than the "readily accessible" and consent exceptions referenced at the top of the statute, *id.* § 2511(1). Second, the argument makes no practical sense. Hinging the viability of a wiretap allegation on the expectations of permissible use cases of the Internet raises more questions than it answers (*e.g.*, What activities are "in the ordinary course of business" when browsing Google Chrome? Would they be tied to Google's terms of service? Do private terms of service offer grounds for prosecution?). Even if the Court was to consider the government's analysis, the government failed to allege in the Indictment that Defendant did not use his device in the ordinary course of business. That omission preserves amici's arguments because defendants would still be forced to rebut allegations after the pleading stage. The government's First Amendment arguments flow from its statutory interpretation, and fail with it too.

that the text of the prohibition expressly incorporates the exceptions, and that the Act's exceptions crucially limit it from reaching common and legal conduct, omitting them does the very violence prohibited by *McArthur*.

The goal of the Wiretap Act, and the entire Electronic Communications Privacy Act ("ECPA"), is to preserve the privacy of truly private communications. *See* S. Rep. No. 99-541, at 2 (1986) ("[The Wiretap Act] is the primary law protecting the security and privacy of business and personal communications . . . ."). Section 2511(1)(a), without its exceptions, cannot define a "cogent offense" because it embroils even the intended recipient of a private communication. It would even embroil an *unwilling* recipient.

C. Holding otherwise would open the floodgates to abusive claims.

As the Court has noted, 4/14/2025 Order at 24 (Doc. 110), it may be true that no one has yet thought to indict someone for merely watching a live broadcast. But if this Court endorses the reading posited by the government, that will surely change. Prosecutors and litigious individuals can and do file frivolous claims, especially if the prima facie elements of a claim have been met. *See* 2000 Fla. Sess. Law Serv. Ch. 2000-174 (H.B. 135) (West) (preamble to Florida's Anti-SLAPP statute noting that SLAPPs "are typically dismissed as unconstitutional, but often not before the defendants are put to great expense, harassment, and interruption of their duties").

This Court should not underestimate the creativity of officials seeking to suppress criticism. The Los Angeles County Sheriff's Department, for example, urged prosecutors to charge a journalist with possession of stolen property for routine reporting on government records.[3] Investigative journalist James Risen recently revealed that the Obama administration threatened to prosecute him under the Sarbanes-Oxley Act for not retaining old reporting notes.[4]

The lack of similar cases under the Wiretap Act can most naturally be attributed to past prosecutors' understanding of the Act as precluding a prima facie case based on the acquisition of any electronic communication. A ruling to the contrary here would change that and invite abuse.

D. Reading the Act's exceptions as elements avoids absurd results.

The Supreme Court has held that a statute should not be construed literally if that would lead to absurd conclusions. *United States v. Bryan*, 339 U.S. 323, 338 (1950).

---

[3] Connor Sheets, *Former Times Reporter Sues Villanueva, L.A County, Alleging 1st Amendment Violation*, L.A. Times (May 27, 2025), https://www.latimes.com/california/story/2025-05-27/former-times-reporter-files-1st-amendment-suit-against-former-sheriff-villanueva-county.

[4] Freedom of the Press Found., *Using Public Records to Fight Government Secrecy and Improve Communities*, at 24:40 (YouTube, streamed June 24, 2025, at 15:00 ET), https://www.youtube.com/watch?v=AHGmEfZEMV8.

An expansive interpretation of the Wiretap Act could flip the default of the American Internet experience from an open web to a closed one. Rather than assuming that we are all allowed to access publicly-available sites and livestreams, it would presume that we *cannot* do so without affirmatively proving an exception covers us. It would allow a plaintiff or prosecutor to force a defendant who merely watches the news, turns on the radio, or participates in a Zoom call to engage in a protracted legal defense to prove that the content was publicly available or that they were the intended recipient. *See Snow v. DirecTV, Inc.*, 450 F.3d 1314, 1321 (11th Cir. 2006) (unless Stored Communication Act required affirmative allegations that website was not accessible to the general public, the "floodgates of litigation would open and the merely curious would be prosecuted"). That task is further complicated by the fact that much of the content that is livestreamed disappears from public view through manual takedowns and automated removals by apps like Snapchat and Instagram Live.

Take the conduct at issue in this case: typing a URL into a web browser and accessing an open, unencrypted website showing a live broadcast. That could cover anything from listening to Supreme Court arguments online to watching a livestream of kittens. It is only the Act's exceptions that prevent the absurd possibility that either could be prosecuted.

Courts have limited their readings of earlier iterations of this law and clarified the requirements of similar laws to avoid absurd results. In 1984, the Kansas Supreme Court considered whether intercepting conversations using cordless telephones—which had been publicly accessible over radio frequency—violated the Wiretap Act. *State v. Howard*, 679 P.2d 197 (Kan. 1984). Because, then, as now, the Act defined "oral communications"—but not "wired communications"—to require a showing of a reasonable expectation of privacy, the court treated the transmissions as "oral communications," for the alternative would have led to absurd instances of Wiretap Act violations. *Id.* at 205.[5]

Recent litigation clarifying the elements of the Computer Fraud and Abuse Act ("CFAA") is also instructive. Courts have found that the statute's language prohibiting acts that "exceed[ ] authorized access," *see* 18 U.S.C. § 1030, must be read narrowly to exclude everyday conduct. *See United States v. Valle*, 807 F.3d 508, 527–28 (2d Cir. 2015); *WEC Carolina Energy Sols., Inc., v. Miller*, 687 F.3d 199, 204–06 (4th Cir. 2012); *United States v. Nosal* (*Nosal I*), 676 F.3d 854, 860 (9th Cir. 2012); *hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1001 (9th Cir. 2019); *Sandvig v. Barr*, 451 F. Supp. 3d 73, 88 (D.D.C.

[5] When ECPA was passed in 1986, this problem was fixed by specifically removing "readily accessible" radio communications from the scope of liability. *See* 18 U.S.C. § 2511(2)(g).

2020), *appeal docketed*, No. 20-5153 (D.C. Cir. May 28, 2020) ("Criminalizing terms-of-service violations risks turning each website into its own criminal jurisdiction and each webmaster into his own legislature."); *Van Buren v. United States*, 593 U.S. 374, 388–89 (2021).

For the same reasons, this Court should clarify that the Act requires prosecutors and plaintiffs to negate public or practical availability as elements.

II. Constitutional Avoidance Requires that the Act's Statutory Exceptions Be Read as Elements Alleged in the Indictment.

Even if the Court is not convinced that a proper reading of the Act requires the exceptions to be read as elements, the doctrine of constitutional avoidance requires the same result. When, as here, a court is confronted with two potential interpretations of a statute and "one of them would create a multitude of constitutional problems, the other should prevail." *Clark v. Martinez*, 543 U.S. 371, 380–81 (2005).

A. Shifting the burden to defendants to establish that an exception applies would raise First Amendment concerns.

A statute that makes accessing publicly-available livestreams presumptively unlawful and shifts the rebuttal burden to a defendant would burden individuals' First Amendment rights in vague and overbroad ways, and chill constitutionally-protected conduct.

1. Imposing the burden of proof on defendants would burden the rights to receive and gather information

Interpreting Sections 2511(2)(d) and (2)(g)(i) as affirmative defenses would encroach on Americans' First Amendment rights to access and receive information. The First Amendment protects the rights of speakers *and* listeners. *Lamont v. Postmaster Gen.*, 381 U.S. 301, 305, 307 (1965). The government "may not, consistently with the spirit of the First Amendment, contract the spectrum of available knowledge." *Griswold v. Connecticut*, 381 U.S. 479, 482 (1965); *First Nat'l Bank of Bos. v. Bellotti*, 435 U.S. 765, 776–77 (1978) (striking down a restriction on corporate electioneering because of its "capacity for informing the public"); *Va. State Bd. of Pharmacy v. Va. Citizens Consumer Council, Inc.,* 425 U.S. 748, 757 (1976) (recognizing consumers' First Amendment "right to receive" advertising); *Island Trees Sch. Dist. v. Pico*, 457 U.S. 853, 867 (1982) (plurality opinion) (recognizing the right to receive information through books in school libraries).

The First Amendment also protects the right to gather information, even if the subjects of that information would not consent. For example, "banning photography or note-taking at a public event would raise serious First Amendment concerns; a law of that sort would obviously affect the right to publish the resulting photograph or disseminate a report derived from the notes. The same is true of a ban on audio and audiovisual recording." *ACLU of Ill. v. Alvarez*, 679 F.3d 583, 595–96 (7th Cir. 2012).

The constitutional right to gather and receive information protects freedom of thought by reinforcing a person's "right to read or observe what he pleases . . . ." *Stanley v. Georgia*, 394 U.S. 557, 565 (1969). It is "clearly vital" for self-governance. *Martin v. City of Struthers*, 319 U.S. 141, 146–47 (1943). And, while people previously relied on public broadcasts to learn about matters of public significance like the moon landing and presidential debates,[6] they now increasingly exercise their rights to gather and access information by accessing livestreams. Livestreams have been key to the public's understanding of everything from updates on election results, breaking news about natural disasters, to Congressional, federal, and state court hearings.[7]

The right to access and gather information also ensures that journalists have enough breathing room to serve society by searching for information of public concern.[8] Journalists often gain access to information in ways that

---

[6] *See, e.g.*, *History of Commercial Radio*, Fed. Commc'ns Comm'n (Oct. 17, 2023), https://www.fcc.gov/media/radio/history-of-commercial-radio; James Jeffrey, *Apollo 11: 'The Greatest Single Broadcast in Television History'*, BBC (July 10, 2019), https://www.bbc.com/news/world-us-canada-48857752; *Watch All the Presidential Debates Since 1960*, PBS NewsHour, https://www.pbs.org/newshour/elections/2020/historic-debates/#2020-1st-biden-trump (last visited June 24, 2025).

[7] *Floor Proceedings*, U.S. Senate, https://www.senate.gov/legislative/floor_activity_pail.htm (last visited June 24, 2025); *Florida Virtual Courtroom Directory*, Fla. Courts, https://courtrooms.flcourts.gov (last visited June 24, 2025); *see also Remote Public Access to Proceedings*, U.S. Courts, https://www.uscourts.gov/court-records/access-court-proceedings/remote-public-access-proceedings (last visited June 24, 2025).

[8] "The protected right to publish the news would be of little value in the absence of sources from which to obtain it." *CBS Inc. v. Young*, 522 F.2d 234, 238 (6th Cir. 1975);

offend the subjects of their reporting—overhearing a conversation at a crowded restaurant or obtaining an audio recording from a whistleblower. *See, e.g.*, *Bartnicki v. Vopper*, 532 U.S. 514, 535 (2001) (radio commentator sued for airing recorded cellphone conversation); *N.Y. Times Co. v. United States* (*The Pentagon Papers*), 403 U.S. 713 (1971) (publication of classified materials). But the First Amendment protects even "surreptitious, confrontational, unscrupulous and ungentlemanly" investigatory tactics as necessary for robust public accountability. *Desnick v. Am. Broad. Cos.*, 44 F.3d 1345, 1355 (7th Cir. 1995). This protection is not limited to the mainstream media—these days, anyone with a smartphone can engage in constitutionally-protected acts of journalism, regardless of whether they call themselves a "journalist." *See Glik v. Cunniffe*, 655 F.3d 78, 83 (1st Cir. 2011) ("[T]he public's right of access to information is coextensive with that of the press.").

Journalists—mainstream and otherwise—rely on livestreaming, both as a means of publishing and as source material. Journalists regularly comb obscure websites for data or investigative scoops. This type of investigation is among "the most powerful techniques for data-savvy journalists who want to

see also People for the Ethical Treatment of Animals, Inc. v. N.C. Farm Bureau Fed'n, Inc., 60 F.4th 815, 829 (4th Cir. 2023) ("The right to gather information plays a distinctly acute role in journalism.").

get the story first, or find exclusives that no else has spotted." Paul Bradshaw, *Scraping for Journalists* (2d ed. 2017) (ebook).

Applying the Act's exceptions as affirmative defenses would encroach on each of these rights. Even if a person who accesses a live public broadcast to report news has a strong affirmative defense, placing the burden on them to prove it would violate the First Amendment.

The Supreme Court has made this clear in several cases. In *Ashcroft v. Free Speech Coalition*, the Supreme Court struck down portions of the Child Pornography Prevention Act of 1996 because it required those who possessed "virtual" pornographic material, protected by the First Amendment, to prove the material was not real. 535 U.S. 234 (2002). The Court noted that "[t]he Government raises serious constitutional difficulties by seeking to impose on the defendant the burden of proving his speech is not unlawful." *Id.* at 255. Similarly, in *Reno v. ACLU*, the Court struck down a law criminalizing the knowing transmission of "obscene or indecent" messages to minors, notwithstanding the availability of defenses, because "the defenses do not constitute the sort of 'narrow tailoring' that will save an otherwise patently invalid unconstitutional provision." 521 U.S. 844, 882 (1997).

Many courts have since followed *Ashcroft*'s logic and not allowed an unconstitutional abridgement of speech to be saved by an affirmative defense. For example, in *Vincenty v. Bloomberg*, 476 F.3d 74 (2d Cir. 2007), the Second

Circuit struck down Section 10–117(c-1) of the New York City Administrative Code—which made the possession of spray paint on another person's property an offense, with defenses available for consent and necessity. *Id.* at 77. As the court explained, "where 'only an affirmative defense is available, speakers may self-censor rather than risk the perils of trial[.]'" *Id.* at 87 (citing *Ashcroft v. ACLU*, 542 U.S. 656, 670–71 (2004)); *see also ACLU v. Mukasey*, 534 F.3d 181, 192–93, 196 (3d Cir. 2008); *Garden Dist. Book Shop, Inc. v. Stewart*, 184 F. Supp. 3d 331, 341 (M.D. La. 2016).[9]

2. Construing the exceptions as affirmative defenses would make the law overbroad and vague

Interpreting the Act's exceptions as affirmative defenses would also raise overbreadth concerns. In *United States v. Stevens*, 559 U.S. 460 (2010), the Court struck down a statute that criminalized the depiction of animal cruelty as overbroad because the "presumptively impermissible applications" of the statute "far outnumber any permissible ones." *Id.* at 481. As in *Stevens*, the impermissible applications of the Wiretap Act here would outnumber the permissible ones if defendants must rely on affirmative defenses.

[9] Conversely, cases that distinguish themselves from *Ashcroft v. Free Speech Coalition* involve statutory prohibitions on non-expressive conduct, transactions, or products that recognize expression-related defenses for a limited set of cases. *See, e.g.*, *O Centro Espirita Beneficiente Uniao Do Vegetal v. Ashcroft*, 389 F.3d 973, 997 (10th Cir. 2004) (Murphy, J., concurring in part and dissenting in part) (declining to enter preliminary injunction against the enforcement of a federal law banning the use of psychotropic substances).

The vast majority of electronic communications are public broadcasts that are "intercepted" by those with a First Amendment right to receive them, either because they are the intended recipients or because the broadcast is available to the general public. The Act's exceptions save those recipients from liability, and must be foregrounded accordingly.

Relegating the Act's exceptions to affirmative defenses would also make the statute vague, creating an "obvious chilling effect on free speech" as a result of the lack of clarity and, because of the Act's criminal sanctions, only making it more likely that "speakers [will] remain silent rather than communicate even arguably unlawful words, ideas, and images." *Reno*, 521 U.S. at 872. "As a practical matter, [these] increased deterrent effect[s], coupled with the risk of discriminatory enforcement of vague regulations, poses great[ ] First Amendment concerns." *Id.* (cleaned up); *see also Grayned v. Rockford,* 408 U.S. 104, 108–09 (1972) ("delegat[ing] basic policy matters to policemen, judges, and juries for resolution on an ad hoc and subjective basis" through a vague law is "impermissibl[e]").

That even an *intended* recipient could be considered to unlawfully "intercept" a communication would make prosecutors and potential criminal defendants alike uncertain of what routine conduct may be prosecuted. And selective enforcement would likely be used against journalists, political dissidents, and other gadflies. Even if the Court has confidence that

prosecutors would be unlikely to indict somebody who has a strong defense, it should "not uphold an unconstitutional statute merely because the Government promised to use it responsibly." *Stevens,* 559 U.S. at 480. Equally, courts must guard against laws that rely on the good judgment of plaintiffs to avoid abuse; indeed, that could be just another name for a chilling effect. "Ubiquitous, seldom-prosecuted crimes invite arbitrary and discriminatory enforcement." *Nosal I*, 676 F.3d at 860. Interpreting the Wiretap Act's exceptions as affirmative defenses enables prosecutors to pick and choose their targets.[10]

3. Construing the elements as affirmative defenses would have widespread chilling effects

This understanding of the Wiretap Act would also cause a significant and entirely rational change in the behavior of Internet users, journalists, and Internet service providers to avoid arrest or costly litigation. As discussed above, *supra* Section I.C, the government's interpretation of the Wiretap Act would unleash frivolous litigation and make the Act a magnet for arbitrary and harassing enforcement actions in the future.

Journalists may not yet have been prosecuted for watching YouTube, but some recent cases are not far off. For example, in 2023, police in Marion

[10] An expansive interpretation also conflicts with the Privacy Protection Act of 1980, which restricts investigations of journalists when the purported crime of which they are accused involves routine newsgathering. 42 U.S.C. § 2000aa(a).

County, Kansas raided the home and office of a news publisher on suspicion that the publisher violated the state's computer crime laws by accessing a government website to verify a news tip.[11]

In another case, a reporter for the St. Louis Post-Dispatch discovered a security flaw in a state website that put thousands of Social Security numbers at risk of disclosure.[12] He alerted the appropriate authorities so they could fix the problem, but the governor called for his prosecution for computer crimes.[13] And the city of Fullerton, California, sued local bloggers under federal and state computer crime laws for reviewing information stored on a city Dropbox page publicly available without a password.[14]

---

[11] *Material Seized in Police Raid of Kansas Newspaper Should Be Returned, Prosecutor Says*, CBS News (Aug. 16, 2023), https://www.cbsnews.com/news/kansas-newspaper-police-raid-marion-county-prosecutor-items-returned. The Marion County prosecutor ordered that the police had to return all seized material for insufficient evidence, *id.*, and the police chief who led the raid was later charged with felony obstruction of justice for his conduct in the subsequent investigation of the events. Emily Mae Czachor, *Ex-Police Chief Who Led Raid on Kansas Newspaper Charged with Obstruction of Justice*, CBS News (Aug. 13, 2024), https://www.cbsnews.com/news/gideon-cody-marion-county-record-raid-kansas-newspaper-charged-obstruction-of-justice.

[12] Jason Hancock, *Claim that Reporter Hacked State Website Was Debunked. Parson Still Says He's a Criminal*, Mo. Indep. (Feb. 23, 2022), https://missouriindependent.com/2022/02/23/claim-that-reporter-hacked-state-website-was-debunked-parson-still-says-hes-a-criminal/.

[13] *Id.* An exhaustive state report eventually found no evidence of criminality. The prosecutor said the law was so vague that it could be abused to criminalize using "a computer to look up someone's information." *Id.*

[14] *See Friends for Fullerton's Future v. City of Fullerton*, No. G044597, 2012 WL 2395554, at *8 (Cal. Ct. App. June 26, 2012).

These cases eventually failed, but only after causing difficulties and expense for the defendants and deterring other journalists. They illustrate the very real risk that a rogue prosecutor would take advantage of an opening that an improper interpretation of the Wiretap Act would create to file an indictment, despite the existence of a strong defense, in order to deter constitutionally-protected journalism.[15]

Moreover, because the Wiretap Act also provides a private right of action, interpreting its exceptions as affirmative defenses would also put a cudgel in the hands of individuals who are unhappy with anyone who shares unflattering information from electronic communications they lawfully accessed. The history of defamation law and the decision of most states, including Florida, to enact anti-SLAPP laws support this likely outcome, as they demonstrate that powerful plaintiffs are often highly motivated to file costly lawsuits against their critics and adversaries, regardless of the merits of their affirmative defenses.

That the Act is likely to be abused against journalists is particularly concerning, for the press disseminates information on matters of public concern and often earns the ire of powerful public figures in the process. *See*

[15] Laws involving computer crimes are prone to abuse because they were drafted using outdated terms that don't quite match the eventual development of the regulated technologies, or how people interact with them. The statutory ambiguities have been used against journalists because of (not despite) their good reporting.

N.Y. Times Co. v. Sullivan, 376 U.S. 254, 270 (1964). To uncover the truth and expose corruption, journalists must often upset government officials and other powerful people. As a result, they are natural targets for novel legal theories or weak criminal charges.

The expense of fighting Wiretap Act charges would also be a huge disincentive to lawful newsgathering and truthful reporting. Journalists are motivated to seek out obscure or abandoned information that others wouldn't be bothered to find. Their newsgathering methods, including scouring technically public but often-ignored websites and livestreams, are more likely to flirt with the most vague and contradictory provisions of the Wiretap Act.

Journalists are not the only actors who are likely to tread cautiously. All content creators would be reluctant to use electronic communications in their social media posts; Zoom meetings would be fraught; and technology platforms might find it "prohibitively expensive" to verify that hosting livestreams does not risk prosecution. *See Reno*, 521 U.S. at 877.

B. Reading the exceptions as elements would avoid the constitutional issue.

Fortunately, there is a natural construction of the Wiretap Act that avoids these constitutional issues—requiring prosecutors to make a prima facie case that the communications in question were not accessible to the public and that defendants did not have consent to access them. *See* 18 U.S.C.

§ 2511(2)(d), (2)(g)(i). Just as the First Amendment requires defamation plaintiffs to "bear the burden of showing that the speech at issue is false" rather than forcing the defendant to prove truth as a defense, *Phila. Newspapers, Inc. v. Hepps*, 475 U.S. 767, 777 (1986), it requires those bringing Wiretap Act cases to allege and prove that the relevant communication was private.

Courts have relied upon the constitutional avoidance canon to interpret the CFAA to avoid similar risks to individuals' First Amendment and due process rights. *See Sandvig*, 451 F. Supp. 3d at 88–89 ("Plaintiffs' First Amendment challenge raises such risks . . . and thus weighs in favor of a narrow interpretation under the avoidance canon."). This Court should do the same here.

III. The Rule of Lenity Also Necessitates Reading the Relevant Sections as Elements of an Offense Rather than as Affirmative Defenses.

The rule of lenity calls for courts to interpret ambiguous criminal statutes narrowly in favor of the defendant. *United States v. Santos*, 553 U.S. 507, 514 (2008). This principle "not only ensures that citizens will have fair notice of the criminal laws, but also that Congress will have fair notice of what conduct its laws criminalize. We construe criminal statutes narrowly so that Congress will not unintentionally turn ordinary citizens into criminals." *Nosal I*, 676 F.3d at 863. To the extent that the status of Act's exceptions as

affirmative defenses or elements is ambiguous, the latter interpretation appropriately narrows the statute at the prima facie stage and provides better notice for all on what is criminalized.

CONCLUSION

For the foregoing reasons, the Court should hold that Sections 2511(2)(d) and (2)(g)(i) state elements of the offense.

Dated: June 27, 2025

Respectfully submitted,

By: /s/ Daniel Tilley

Daniel Tilley (Fla. Bar No. 102882)
Counsel of Record
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF FLORIDA
4343 W. Flagler Street, #400
Miami, FL 33134
(786) 363-2714
dtilley@aclufl.org

Counsel for Amici Curiae

Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111
(415) 343-0758
jgranick@aclu.org

Vera Eidelman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
(212) 549-2500
veidelman@aclu.org

Aaron Mackey
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333
amackey@eff.org

Bobby Block
FLORIDA FIRST AMENDMENT FOUNDATION
317 E. Park Avenue
Tallahassee, FL 32301
(850) 222-3518
bblock@floridafaf.org

Yanni Chen
Nora Benavidez
FREE PRESS
1025 Connecticut Avenue NW
Suite 1110
Washington, DC 20036
(202) 265-1490
ychen@freepress.net
nbenavidez@freepress.net

Seth Stern
FREEDOM OF THE PRESS FOUNDATION
49 Flatbush Avenue, #1017
Brooklyn, NY 11217
(510) 995-0780
seth@pressfreedomfoundation.org

Jane Bambauer
UNIVERSITY OF FLORIDA
LEVIN COLLEGE OF LAW
309 Village Drive
PO Box 117620
Gainesville, FL 32611
(352) 273-32611
janebambauer@ufl.edu