Vol. 117
Northwestern University Law Review

PRESERVING PRIVILEGE: DEVELOPING A SOUND LITIGATION STRATEGY FOR PRISON WIRETAPPING CASES

Daniel J. Cummins

ABSTRACT—The attorney–client privilege is the oldest and most storied privilege in the United States common law. The justifications for the preservation of the privilege compound when applied to incarcerated individuals who wish to speak with their counsel privately over the phone to organize their criminal defense, appeal a judgment, or work through negotiations with the government. However, in recent years, private telecommunications providers operating in jails and prisons have continually violated that privilege by recording prisoners' calls with their attorneys. Plaintiffs have taken to the courts to litigate these wrongs but have enjoyed limited and disparate degrees of success. This Note explores one possible civil cause of action available to prisoners and their attorneys in these situations: the Federal Wiretap Act. Specifically, it analyzes and rebuts defendants' most prevalent defenses. In doing so, it offers a litigation roadmap to plaintiffs who have been harmed by these predatory recording practices and wish to hold the telecommunications companies responsible for their actions.

AUTHOR—J.D. Candidate, Northwestern Pritzker School of Law, 2023; B.S., Indiana University, 2017. I owe a deep debt of gratitude to every member of the *Northwestern University Law Review Online* team for their thoughtful work on this Note and support over the past year. Thanks as well to Alan Mills, Executive Director of the Uptown People's Law Center, for his course on Prisons and Prisoners' Rights, which provided me with the opportunity to write on this topic. To Maurice Possley, for his careful copyediting. Finally, a very special thank you to my grandfather, Robert Cummins. Not only did he inspire this Note, but he has served as the best guidepost and confidant that I could ask for as I pursue a career in the law.

INTRODUCTION

In 2015, an anonymous hacker released a vast collection of prisoner phone calls recorded by a private communications company while under contract with jails and prisons across the United States.[1] The company, Securus Technologies (Securus), is the second largest prison and jail telecommunications provider, serving some 3,400 facilities.[2] Securus recorded more than seventy million calls between winter 2011 and spring 2014, and at least 14,000 of the recorded telephone calls were between

[1] Jordan Smith & Micah Lee, *Not So Securus: Massive Hack of 70 Million Prisoner Phone Calls Indicates Violations of Attorney-Client Privilege*, INTERCEPT (Nov. 11, 2015, 11:43 AM), https://theintercept.com/2015/11/11/securus-hack-prison-phone-company-exposes-thousands-of-calls-lawyers-and-clients/ [https://perma.cc/VDL9-CHBW].

[2] *See Facilities We Serve*, SECURUS TECHS., https://securustech.online/#/facilities-we-serve [https://perma.cc/5Q4W-ETXU]; Laurence Darmiento, *Troubled Companies Made Him Billions. A Prison Phone Investment Made Him Enemies*, L.A. TIMES (Sept. 5, 2019, 5:00 AM), https://www.latimes.com/business/story/2019-09-05/la-fi-tom-gores-securus-prison-phone-mass-incarceration [https://perma.cc/DBR2-YBFK]. Not only is Securus one of the biggest prison telecommunications providers in the country, but it has also become a symbol in pop culture, being mentioned in modern hip-hop songs by rappers such as Polo G. POLO G, *Through Da Storm*, *on* DIE A LEGEND (Columbia Records 2019) ("Talkin' to my lil' sister, phone calls through Securus."). However, this Note is not applicable to Securus alone. The largest prison telecommunications provider, ViaPath Technologies (formerly Global Tel Link), has also been accused of similar unlawful recording of prisoner–attorney calls. *See* JIM BAKER, PRIV. EQUITY STAKEHOLDER PROJECT, AMERICAN SECURITIES' BIG BET ON PRISON PHONE CALLS 2 (2020), https://pestakeholder.org/wp-content/uploads/2020/02/American-Securities-Big-Bet-on-Prison-Phone-Calls-PESP-022020.pdf [https://perma.cc/6W65-73BV] ("GTL . . . is the country's largest provider of correctional telephone systems, video-calling systems, financial and electronic equipment to incarcerated individuals."); *Prison Phone Companies Recording Attorney-Client Calls*, EQUAL JUST. INITIATIVE (Jan. 7, 2022), https://eji.org/news/prison-phone-companies-recording-attorney-client-calls/ [https://perma.cc/E39S-FA72] ("GTL allegedly recorded phone calls with attorneys in Florida, California, and Maine . . . ."). The analysis this Note offers is broad, extending to any entity that intercepts attorney–client communications from prison phone systems.

inmates and their attorneys.[3] Of these 14,000 calls, there was "a strong indication" that many were protected by the attorney–client privilege.[4]

As early as 2013—two years before the data leak—criminal defense attorneys in Austin, Texas became aware that Securus was recording their conversations with clients at the Travis County Jail (TCJ) and Travis County Correctional Center (TCCC).[5] In 2014, these attorneys, along with the Austin Lawyers Guild,[6] filed a class action complaint in the Western District of Texas alleging that Securus recorded privileged calls between detainees and their attorneys at TCJ and TCCC and, in many cases, inadvertently turned over these recordings to local prosecutors.[7] According to the complaint, these actions violated the Federal Wiretap Act, the Texas Wiretap Act, and the U.S. Constitution.[8]

Between 2014 and today, there have been at least five other class action complaints in federal district courts across the country accusing prison telecommunications providers of violating wiretapping statutes.[9] While phone call recording is the norm in prisons,[10] these complaints allege that attorney calls fall outside the scope of what telecommunications providers

---

[3] Smith & Lee, *supra* note 1 ("The mass recording of detainee calls was originally rationalized as improving safety within a facility – a way to hedge against contraband being brought in, to ferret out escape attempts or potentially violent uprisings, and to curb the possibility of witness tampering or intimidation.").

[4] *Id*.

[5] *See* Plaintiffs' Amended Class Action Complaint paras. 11–20, Austin Laws. Guild v. Securus Techs., Inc., No. 1:14-cv-00366-LY, 2014 WL 5343347 (W.D. Tex. July 23, 2014).

[6] The Austin Lawyers Guild is a nonprofit organization which includes a substantial number of criminal defense attorneys. The organization's purpose, according to its bylaws, is to "promote the public interest, civil rights, and social justice." *See id*. para. 4.

[7] *Id*. paras. 16–18.

[8] *Id*. paras. 32–39. Specifically, the complaint alleged violations of the First, Fourth, Fifth, and Sixth Amendments of the Constitution.

[9] *See* Pratt v. Securus Techs., Inc., No. 1:20-cv-00295-JDL, 2021 WL 1725936 (D. Me. Apr. 30, 2021) (order on defendant's motion to dismiss finding prisoners and attorneys failed to allege facts sufficient to support a finding of intent under the Federal Wiretap Act); Romero v. Securus Techs., Inc., 331 F.R.D. 391 (S.D. Cal. 2018) (partial ruling on plaintiffs' motion for summary judgment, allowing the case to proceed alleging violations of the California Invasion of Privacy Act (CIPA)); Crane v. Corr. Corp. of Am., No. 16-CV-947, 2016 WL 11703731 (W.D. Mo. Aug. 31, 2016) (plaintiff's complaint alleging violations of state wiretap statutes); Huff v. CoreCivic, Inc., No. 17-2320-JAR-JPO, 2018 WL 1175042 (D. Kan. Mar. 5, 2018) (dismissing Securus's motion for judgment on the issue of whether prisoner calls fell within the business-extension exception to the Federal Wiretap Act); Bliss v. CoreCivic, Inc., No. 2:18-cv-01280-JAD-EJY, 2022 WL 167584 (D. Nev. Jan. 14, 2022) (denying defendant's motion to dismiss, including on the issues of intent and business-use exception).

[10] Ken Armstrong, *A Phone Call from Jail? Better Watch What You Say*, THE MARSHALL PROJECT (Sept. 4, 2015, 7:15 AM), https://www.themarshallproject.org/2015/09/04/a-phone-call-from-jail-better-watch-what-you-say [https://perma.cc/Y9X5-CFHH] ("In jail or prison, rules governing privacy tend to be suspended. With rare exception—for example, inmate-attorney communications— conversations can be monitored.")

can and should record. Plaintiffs argue that recording attorney calls not only violates the attorney–client privilege, but also the providers' express policies.[11] Regardless of how or why these recordings continue to happen, attorneys and prisoners alike have taken to the courts to ask that telecommunications providers be held liable for their actions.

Despite the increase in litigation, these cases are often dismissed or settled in advance of trial,[12] leading to a dearth of substantive case law. This lack of final judgments on the merits raises questions about what criminal and civil violations occur when telecommunications providers record calls between attorneys and imprisoned clients. Further, while legal scholarship has long discussed the attorney–client privilege in prison, especially as it relates to in-person client meetings and communications by mail or email,[13] there is a noticeable lack of scholarship on phone calls between prisoners and their attorneys and what recourse these individuals have when their calls are recorded.

This Note examines one civil cause of action that prisoners and their attorneys can bring under the Federal Wiretap Act. Part I of this Note introduces the relevant provisions of the Act. It outlines the remedies available to plaintiffs who sue under the Act, how the Act addresses privileged communications, and the statutory elements and exceptions relevant to the analysis. Part II addresses standing. It overviews the attorney–

---

[11] *See, e.g.*, Plaintiffs' Amended Class Action Complaint para. 15, *Austin Laws. Guild*, 2014 WL 5343347 (referencing Securus's policies against recording inmates' phone and video calls with their attorneys); *Rules and Regulations*, SECURUS TECHS., https://securustech.net/tdcj/#tdcj-rules-and-regulations [https://perma.cc/E672-YQNX] ("All calls, except to [the detainee's] Attorney of Record, are subject to monitoring and recording."); *see also* Gregory Sisk, Michelle King, Joy Nissen Beitzel, Bridget Duffus & Katherine Koehler, *Reading the Prisoner's Letter: Attorney-Client Confidentiality in Inmate Correspondence*, 109 J. CRIM. L. & CRIMINOLOGY 559, 568 (2019) ("The inmate is in a most vulnerable position when it comes to attorney-client confidentiality because she is entirely dependent on the prison establishment to confidentially transmit correspondence to and from her counsel, allow unmonitored telephone calls with counsel, and arrange for attorney-client meetings in a confidential setting.").

[12] *See, e.g.*, *Pratt*, 2021 WL 5094907, at *5 (dismissing complaint for insufficiently alleging intent); Dan Margolies, *Leavenworth Inmates Reach $1.45 Million Settlement over Taped Attorney-Client Phone Calls*, KCUR (Aug. 26, 2019, 11:32 AM) https://www.kcur.org/news/2019-08-26/leavenworth-inmates-reach-1-45-million-settlement-over-taped-attorney-client-phone-calls [https://perma.cc/7DGQ-MBV5] (discussing settlement reached in *Huff v. CoreCivic*).

[13] *See* Elizabeth Choi, *The Pandemic of Intrusion into Privileged Communications Between Incarcerated Clients and Their Attorneys*, 34 GEO. J. LEGAL ETHICS 831, 832 (2021); Sisk et al., *supra* note 11, at 565; Gregory R. Steele, *You've Got Legal Mail: Applying Constitutional Protections to Attorney–Inmate E-Mail Communications*, 50 GA. L. REV. 947, 952 (2016); Christopher J. Milazzo, Note, *When it Comes to Privilege, You're Better Off Dead: Protecting Attorney-Client Communications Sent Through Prison Email Systems*, 25 CORNELL J.L. & PUB. POL'Y 269, 271 (2015); Amelia H. Barry, Comment, *Inmates' E-Mails with Their Attorneys: Off-Limits for the Government?*, 64 CATH. U. L. REV. 753, 754 (2015); Danielle Burkhardt, Comment, *Read, White, and Blue: Prosecutors Reading Inmate Emails and the Attorney-Client Privilege*, 48 J. MARSHALL L. REV. 1119, 1122 (2015).

client privilege and how a violation of the privilege can provide an adequate basis for an injury-in-fact argument for current and former prisoners. This Part also discusses theories of harm for attorneys and other relevant considerations for choosing plaintiffs in a Federal Wiretap Act case, with a focus on the Prison Litigation Reform Act (PLRA). Part III analyzes the particulars of the Federal Wiretap Act as applied to the attorney–prisoner context. It focuses on the three statutory exceptions that companies have raised as defenses to Federal Wiretap Act claims: intent, consent, and the business-extension exception; the Part then rebuts those arguments and suggests a roadmap for plaintiffs who wish to bring these suits. The Note concludes by explaining how the Federal Wiretap Act provides an adequate civil remedy for the unauthorized recording of prisoner–attorney phone calls.[14]

I. IMPORTANT ELEMENTS OF THE FEDERAL WIRETAP ACT

Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (hereinafter "Federal Wiretap Act") "governs private and governmental nonconsensual electronic surveillance."[15] The statute emerged after a long history of courts grappling with government surveillance of private communications, and it sought to reconcile two competing interests: (1) law enforcement officials' interest in intercepting pertinent information for ongoing investigations and (2) the public's interest in privacy.[16]

The relevant operative provisions of the Federal Wiretap Act provide:

> (1) [A]ny person who—
>
> > (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication . . .
> >
> > (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral, or electronic communication in violation of this subsection . . .

[14] This Note will often refer to "prisons" and "prisoners." These words should be taken to mean all individuals incarcerated in either a jail (which is typically run by the county and houses individuals who are awaiting final adjudication of their criminal charges) or a prison (typically a long-term state or federal facility for individuals who have already been convicted of crime(s)).

[15] Michael Goldsmith & Kathryn Ogden Balmforth, *The Electronic Surveillance of Privileged Communications: A Conflict in Doctrines*, 64 S. CAL. L. REV. 903, 904 (1991); 18 U.S.C. §§ 2510–2521 (1968).

[16] Goldsmith & Balmforth, *supra* note 15, at 904.

> shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5).[17]

Further, § 2520 creates a civil cause of action for violations of the statute. It states, "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate."[18]

While the Federal Wiretap Act prevents the unlawful interception of private communications, it also enables the government and authorizes private entities to intercept these communications in certain circumstances. For example, the interception, use, or disclosure of a wire communication does not violate the Act in cases where the government has received a warrant to record an individual's conversations or when one party consents to the recording.[19] Moreover, key features of the Federal Wiretap Act, namely its intent standard and liability exceptions, limit opportunities for redress for otherwise unlawful surveillance.

For privileged communications, such as those between attorneys and clients seeking legal advice, the Act provides limited protections. Section 2517 of the Act states that "[n]o otherwise privileged wire, oral, or electronic communication intercepted in accordance with, or in violation of, the

---

[17] 18 U.S.C. § 2511(1)(a), (c). "'[P]erson' means any employee, or agent of the United States or any State or political subdivision thereof, and any individual, partnership, association, joint stock company, trust, or corporation." 18 U.S.C. § 2510(6). This definition plainly implicates private telecommunications firms. Whether it also includes state or local governments is less clear. *Compare* Adams v. City of Battle Creek, 250 F.3d 980, 985–86 (6th Cir. 2001) (holding nonfederal governmental entities may be held liable for civil violations of the Federal Wiretap Act), *with* Seitz v. City of Elgin, 719 F.3d 654, 660 (7th Cir. 2013) (holding nonfederal governmental entities may not be held liable for civil violations of § 2511(1) of the Federal Wiretap Act). The litigation strategy in this paper is geared toward suits against private telecommunications providers such as Securus and ViaPath.

[18] 18 U.S.C. § 2520(a). Section § 2520(b) of the Act provides for three primary forms of relief: "preliminary and other equitable or declaratory relief . . . damages . . . [and] a reasonable attorney's fee and other litigation costs." As a threshold matter, "[i]t is firmly established that the Federal Wiretap Act applies in a prison or detention center and inmates are entitled to notice if their calls are being recorded." Christina Santos, Comment, *An Analysis of* Austin Lawyers Guild v. Securus Technologies, Inc.*: The Constitutional and Ethical Implications of Using Illegally Recorded Attorney–Client Telephone Conversations as Derivative Evidence*, 6 ST. MARY'S J. LEGAL MALPRACTICE. & ETHICS 304, 315 (2016) (citing *Adams*, 250 F.3d at 984–85 (holding even prisoners are entitled to some notice that their calls are being monitored by the facility or another agency)); United States v. Amen, 831 F.2d 373, 378 (2d Cir. 1987) (stating 18 U.S.C. § 2510 clearly applies to prison monitoring). This baseline undercuts any attempt to suggest that the statute does not reach prisoner-plaintiffs who wish to bring claims under the Federal Wiretap Act in state or federal court.

[19] *See* 18 U.S.C. §§ 2511(2)(a)(ii), (c)–(d). None of the cases discussed in this Note involve a situation where a telecommunications provider, or a jail or prison, has obtained a warrant for the interception of attorney–client calls; it is only mentioned here as an illustration of another exception included in the Act beyond those which are discussed in greater detail.

provisions of this chapter shall lose its privileged character."[20] This provision does not immunize privileged communications from interception in the first place; "[r]ather, it allows the person entitled to assert the privilege to move to avoid disclosure of that intercepted conversation."[21] On its face, this distinction seems fatal to the suits brought by prisoners and attorneys such as those in the *Austin Lawyers Guild* litigation. If the only remedy is to prevent disclosure of privileged evidence to adverse parties, then a lawsuit asking for damages would clearly lose.

But this reading of the statute ignores other relevant provisions contained elsewhere in the Act. Under the Act's catchall liability provision, if *any* communications are intercepted "in violation of . . . [the] chapter," plaintiffs can proceed with a civil action under the Federal Wiretap Act and seek injunctive and monetary relief.[22] This language does not differentiate between privileged and nonprivileged communications—the relevant inquiry instead turns on whether the interception of a communication, whatever its characteristics, violates the Act. Violations of the Act in turn depend on whether all of the statutory elements are met and whether a statutory exception does or does not apply to preclude an interception from liability. This Note asserts that privileged communications possess inherent features—as well as special treatment under the telecommunications providers' own internal policies—which make the Federal Wiretap Act's exceptions less likely to apply upon their interception. The interception of a prisoner's privileged communications can therefore provide a basis for monetary and injunctive relief assuming the plaintiff can establish all of the Federal Wiretap Act's statutory elements, most notably, intent.

For this Note's purposes, the Federal Wiretap Act's most relevant element is intent. Section 2511 indicates that anyone who "*intentionally* intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication" violates the statute.[23] Generally, the intent required to establish civil liability under the Federal Wiretap Act has been interpreted—based on legislative history—to mean "purposeful conduct."[24] Before 1986, § 2511 indicated that

---

[20] 18 U.S.C. § 2517(4).

[21] NAT'L WIRETAP COMM'N, ELECTRONIC SURVEILLANCE: REPORT OF THE NATIONAL COMMISSION FOR THE REVIEW OF FEDERAL AND STATE LAWS RELATING TO WIRETAPPING AND ELECTRONIC SURVEILLANCE 95 (1976).

[22] 18 U.S.C. § 2517(4); *see* 18 U.S.C. § 2520(b) (outlining appropriate relief for violations of the Federal Wiretap Act).

[23] 18 U.S.C. § 2511(1)(a) (emphasis added).

[24] Kristine Cordier Karnezis, Annotation, *Construction and Application of Provision of Omnibus Crime Control and Safe Streets Act of 1968 (18 U.S.C.A. § 2520) Authorizing Civil Cause of Action by*

a person must "willfully" commit these acts to violate the statute.[25] "Willfully" was generally understood "to denote at least a voluntary, intentional violation of, and perhaps also a reckless disregard of, a known legal duty."[26] Thus, under this interpretation, a violation of the Federal Wiretap Act required an offender to know his conduct was unlawful and to have proceeded with the interception anyway.[27] Congress amended the statute in 1986 to "dilute the standard of proof from willfulness to mere intent" such that "a defendant who actually intercepts a conversation in a prohibited fashion need not be proved to have known his conduct was illegal."[28] However, as discussed in Part III, whether intent is satisfied in the typical prison wiretapping case remains far from settled.

The first relevant exception to the Federal Wiretap Act is consent. Section 2511(2)(d) of the statute states it "shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication . . . where one of the parties to the communication has given prior consent to such interception."[29] Courts in circuits across the country have held that this exception also includes instances of implied consent.[30] For example, the D.C. Circuit Court of Appeals articulated that implied consent is consent that can be inferred "from surrounding circumstances indicating that the [party] knowingly agreed to the surveillance."[31] Thus, the idea of notice that calls will be recorded, monitored, or otherwise intercepted is critical to a consent argument in the prison context.[32]

Person Whose Wire, Oral, or Electronic Communication Is Intercepted, Disclosed, or Used in Violation of Act, 164 A.L.R. Fed. 139 § 12 (2000).

[25] 18 U.S.C. § 2511(1) (1982) (pre-1986 legislation) (current version at 18 U.S.C. § 2511(1)(a)).

[26] Citron v. Citron, 722 F.2d 14, 16 (2d Cir. 1983), *cert. denied*, 466 U.S. 973 (1984).

[27] *See* Malouche v. JH Mgmt. Co., 839 F.2d 1024, 1026 (4th Cir. 1988) (holding that a reasonable jury could not find the defendant had acted "willfully" without evidence the defendant had knowledge that the alleged wiretap violated a legal duty).

[28] Earley v. Smoot, 846 F. Supp. 451, 453 (D. Md. 1994).

[29] 18 U.S.C. § 2511(2)(d).

[30] *See, e.g.*, Campiti v. Walonis, 611 F.2d 387, 394 (1st Cir. 1979) (finding no implied consent in a Federal Wiretap Act case); Griffin v. City of Milwaukee, 74 F.3d 824, 827 (7th Cir. 1996) (discussing the circumstances surrounding recordings that amounted to consent); Deal v. Spears, 980 F.2d 1153, 1157 (8th Cir. 1992) ("Although constructive consent is inadequate, actual consent may be implied from the circumstances."); Watkins v. L.M. Berry & Co., 704 F.2d 577, 581 (11th Cir. 1983) (stating that intent may be implied in Federal Wiretap Act cases but must not be done "cavalierly"); Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998) (noting that implied consent in a Federal Wiretap Act case is generally an issue of fact that courts should not decide on summary judgment).

[31] *Berry*, 146 F.3d at 1011 (citing Griggs–Ryan v. Smith, 904 F.2d 112, 117 (1st Cir. 1990)); *see also Griggs–Ryan*, 904 F.2d at 118 (discussing how inmate who was notified of his calls being recorded impliedly consented to such recording by taking the calls).

[32] *See Berry*, 146 F.3d at 1011 ("The key question in such an inquiry obviously is whether parties were given sufficient notice.").

Finally, the so-called business-extension exception manifests itself under the definition of "electronic, mechanical, or other device" located in § 2510(5).[33] That definition stipulates that an "electronic, mechanical, or other device" does *not* include "any telephone or telegraph instrument, equipment or facility, or any component thereof . . . being used by a provider of wire or electronic communication service in the ordinary course of its business."[34] Consequently, telecommunications providers argue that their recordings fall outside the scope of the statute because they operate prison phone systems as a part of their everyday business.[35]

For the most part, intent, consent, and the business-extension exception take center stage in complaints and motions to dismiss in these Federal Wiretap Act cases. However, plaintiffs must first articulate an argument on how they have been harmed to have standing to sue. After all, if recorded conversations do not "lose [their] privileged character,"[36] what does it matter that they are recorded in the first place? None of the recordings can be used in ongoing or future criminal prosecutions and plaintiffs only suffer an intangible, dignitary harm. At least so a telecommunications provider might say. This argument introduces important questions related to federal standing doctrine and the scope of the attorney–client privilege.

II. STANDING AND THE ATTORNEY–CLIENT PRIVILEGE

Plaintiffs in prison wiretapping cases must have a right to sue in the first place. This Part not only outlines who has that right and why they have it but also suggests an ideal class of plaintiffs in a Federal Wiretap Act case.

First, assuming a class of plaintiffs wishes to bring their action in federal court, "every class member must have Article III standing"[37] before moving forward with their substantive arguments on liability.[38] To establish standing, a plaintiff must show three elements: they suffered an injury in fact, the injury is fairly traceable to the defendant's challenged conduct, and the injury will be redressed by a favorable decision.[39]

Defendants regularly challenge standing at the pleading phase through a Rule 12(b)(6) motion to dismiss. When assessing such challenges, circuit

---

[33] *See* 18 U.S.C. §§ 2510(5)–2510(5)(a).

[34] *Id.*

[35] *See* Huff v. CoreCivic, Inc., No. 17-2320-JAR-JPO, 2018 WL 1175042, at *3 (D. Kan. 2018).

[36] 18 U.S.C. § 2517(4).

[37] TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2208 (2021).

[38] *See* Raines v. Byrd, 521 U.S. 811, 818 (1997) ("One element of the case-or-controversy requirement is that [plaintiffs], based on their complaint, must establish that they have standing to sue."); Note, *Standing in the Mud:* Hein v. Freedom from Religion Foundation, Inc., 42 AKRON L. REV. 1277, 1279 (2009) ("Plaintiff standing is [an] essential element[] needed for a case to be justiciable.").

[39] Friends of the Earth, Inc. v. Laidlaw Env't. Servs. (TOC), Inc., 528 U.S. 167, 180–81 (2000).

courts apply the plausibility standard that applies to a Rule 12(b)(6) motion.[40] Under this standard, the plaintiff "bears the burden of establishing sufficient factual matter to plausibly demonstrate his standing to bring the action."[41] In making their determinations, a federal judge will assume that the plaintiff's factual allegations are true, ignore merely conclusory statements, and then draw on their "experience and common sense" to decide whether the plaintiff's allegations have facial plausibility.[42]

If injury in fact is satisfied, then the second and third elements of standing would clearly follow because defendants cause the injury by recording prisoner–attorney phone calls, and the court can redress the injury with damages for plaintiffs, including former prisoners, and injunctive relief for plaintiffs who presently experience harm. Thus, defendants commonly challenge the first element of standing, injury in fact.[43] This challenge is unavailing as applied to both prisoner and attorney plaintiffs.[44]

A prisoner plaintiff's injury-in-fact argument rests primarily on the violation of their attorney–client privilege. Prisoner plaintiffs rely on the attorney–client privilege for injury-in-fact arguments because the Supreme Court in *Spokeo* held that "Article III standing requires a concrete injury even in the context of a statutory violation."[45] In other words, prisoner plaintiffs must do more than plausibly allege a statutory violation of the Federal Wiretap Act. They must show that the violation caused an "'invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'"[46]

Before assessing whether a violation of the attorney–client privilege constitutes an injury in fact, it is important to determine whether prisoner–

---

[40] *See, e.g.*, Hochendoner v. Genzyme Corp., 823 F.3d 724, 730 (1st Cir. 2016) (applying "the plausibility standard applicable under Rule 12(b)(6) to standing determinations at the pleading stage"); Silha v. ACT, Inc., 807 F.3d 169, 173–74 (7th Cir. 2015) (stating that courts apply the "same analysis" to making determinations of standing and adequately stating a claim); *In re* Schering Plough Corp. Intron/Temodar Consumer Class Action, 678 F.3d 235, 243–44 (3d Cir. 2012) (explaining that courts apply the same standard of review on challenges to standing and failure to state a claim); White v. United States, 601 F.3d 545, 551–52 (6th Cir. 2010) (noting that, at the pleading stage, the elements of standing must be supported "in the same way" as stating a claim that is plausible); FED. R. CIV. P. 12(b)(6).

[41] *Hochendoner*, 823 F.3d at 731.

[42] Ashcroft v. Iqbal, 556 U.S. 662, 663–64 (2009); *see* Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555–56 (2007).

[43] *See* Motion to Dismiss of Defendant Securus Technologies, LLC at 19, Pratt v. Securus Techs., Inc., No. 1:20-cv-00295-JDL, 2021 WL 1725936 (D. Me. Apr. 30, 2021) (arguing plaintiffs failed to allege sufficient facts to show that recordings amounted to "any concrete harm . . . .").

[44] For largely PLRA-related reasons discussed later, it appears that former prisoners may be best positioned to bring these lawsuits. Where this Note uses the term "prisoner plaintiffs" it should be understood to encompass both currently and formerly incarcerated individuals.

[45] Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016).

[46] *Id.* at 339 (quoting Lujan v. Defs. of Wildlife, 504 U.S. 555, 560 (1992)).

attorney calls are privileged. The basic formula for the attorney–client privilege is as follows:

> (1) Where legal advice of any kind is sought (2) from a professional legal adviser in his capacity as such, (3) the communications relating to that purpose, (4) made in confidence (5) by the client, (6) are at his instance permanently protected (7) from disclosure by himself or by the legal adviser, (8) except the protection be waived.[47]

While there are narrow limitations to the attorney–client privilege, the privilege generally extends to instances when a client seeks legal advice from his counsel. Under the Federal Rules of Evidence, even inadvertent disclosures of communications that would otherwise be subject to the attorney–client privilege do not waive the privilege, since "waiver[s] must be made intentionally."[48] Thus, when a prisoner's call with an attorney is inadvertently recorded, that communication is still privileged.

The attorney–client privilege is equally, if not more, important, to individuals facing criminal charges or who are currently incarcerated. For criminal defendants' counsel to be effective within the meaning of the Sixth Amendment, "there must be confidence and trust between the attorney and the client."[49] The attorney–client privilege applies to confidential communications between prisoners and their attorneys, provided the communications involve prisoners who seek legal advice.[50] Individuals in pretrial detention who face criminal charges have a right to counsel to

---

[47] Santos, *supra* note 18, at 308; *see also* Upjohn Co. v. United States, 449 U.S. 383, 389 (1981) ("[The attorney–client privilege's] purpose is to encourage full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and administration of justice.").

[48] Santos, *supra* note 18, at 309; *see* FED. R. EVID. 502. The Supreme Court has recognized that the attorney–client privilege exists between prisoners and their attorneys; in other words, incarceration does not extinguish the protections the privilege provides. *See* Wolff v. McDonnell, 418 U.S. 539, 576 (1974).

[49] *See* Santos, *supra* note 18, at 310; *see also* U.S. CONST. amend. VI ("In all criminal prosecutions, the accused shall enjoy the right . . . to have the Assistance of Counsel for his defence."); Lanza v. New York, 370 U.S. 139, 143–44 (1962) ("[E]ven in a jail, or perhaps especially there, the relationships which the law has endowed with particularized confidentiality must continue to receive unceasing protection . . . ."); United States v. Levy, 577 F.2d 200, 209 (3d Cir. 1978) ("Free two-way communication between client and attorney is essential if the professional assistance guaranteed by the sixth amendment is to be meaningful.").

[50] *See* Fisher v. United States, 425 U.S. 391, 403 (1976) (limiting the attorney–client privilege to protect only communications made to obtain informed legal advice); AM. BAR ASS'N, ABA STANDARDS FOR CRIMINAL JUSTICE PROSECUTION FUNCTION AND DEFENSE FUNCTION 149–50 (3rd ed. 1993) ("Without [confidentiality], the client may withhold essential information from the lawyer. Thus, important evidence may not be obtained, valuable defenses neglected, and, perhaps most significant, defense counsel may not be forewarned of evidence that may be presented by the prosecution.").

organize their defense and discuss potential plea bargains.[51] Prisoners who have already been convicted on criminal charges may need to speak with their counsel to prepare direct appeals or discuss defenses to new charges that could have arisen during their incarceration.[52] In all of these instances, inmates are seeking legal advice—for an ongoing defense, appeal, or other issue—and the prisoner has an obvious reason for wishing those communications to be made in confidence.[53] Thus, prisoner–attorney phone calls are privileged.

Moreover, when a prisoner's phone calls with his attorney are intercepted, he has suffered a concrete and particularized injury. Applying the 12(b)(6) standard on a motion to dismiss, the Southern District of California found that prisoner plaintiffs did satisfy the injury-in-fact requirement.[54] In that case, defendant Securus argued that allegations of a bare statutory violation were insufficient to establish injury in fact under *Spokeo*.[55] The district court rejected that argument, particularly because the statutory violations at issue in a wiretap case involve specific, legally-protected interests such as the right to privacy.[56] Further, the court acknowledged that when plaintiffs also allege violations of the attorney–client privilege, their alleged harm is plenty strong to withstand a motion to dismiss.[57] As such, prisoner plaintiffs whose privileged calls are recorded suffer particularized injuries that jeopardize their privacy rights and also their

---

[51] *See* Julie B. Nobel, *Ensuring Meaningful Jailhouse Legal Assistance: The Need for a Jailhouse Lawyer-Inmate Privilege*, 18 CARDOZO L. REV. 1569, 1575 (1997).

[52] *Id.*

[53] Pratt v. Securus Techs., Inc., No. 1:20-cv-00295-JDL, 2021 WL 1725936 at *4 (D. Me. Apr. 30, 2021) (drawing on experience and common sense to find recorded calls of inmates speaking with their attorneys violated the attorney–client privilege).

[54] Romero v. Securus Techs., Inc., 216 F. Supp. 3d 1078, 1089 (S.D. Cal. 2016). While the *Romero* case was based on a violation of the California Invasion of Privacy Act (CIPA), not the Federal Wiretap Act, the analysis still holds. In both Federal Wiretap Act cases and lawsuits arising under analogous state statutes, the court looks beyond the statutory violation to the underlying injury. In both instances, this injury is a violation of privacy and the attorney–client privilege. *See, e.g.*, *In re* Facebook, Inc. Internet Tracking Litigation, 956 F.3d 589, 598 (9th Cir. 2020).

[55] *Romero*, 216 F. Supp. 3d at 1087.

[56] *Id.* at 1088–89. The court's reasoning in *Romero* indicates that arguments on breach of the attorney–client privilege may be superfluous for an injury-in-fact argument. *Id.* at 1089. Circuit courts have found that violations of privacy amount to concrete injury in other contexts as well. For example, in Telephone Consumer Protection Act cases, courts have compared the receipt of unwanted phone calls and text messages to more "traditional claims for 'invasions of privacy, intrusion upon seclusion, and nuisance [which] have long been heard by American courts'" in justifying findings of concrete injury. Susinno v. Work Out World Inc., 862 F.3d 346, 351 (3d Cir. 2017) (quoting Van Patten v. Vertical Fitness Grp., LLC, 847 F.3d 1037, 1043 (9th Cir. 2017)).

[57] *Romero*, 216 F. Supp. 3d at 1089 ("The alleged harm to all Plaintiffs—an invasion of their privacy rights—coupled with the additional harm . . . of forfeiting the protections of the attorney-client privilege, constitute a concrete and particularized injury that is actual and imminent.").

attorney–client privilege, one of the oldest and most well-established privileges in American common law.[58]

Attorney plaintiffs also have strong arguments in support of why they suffer an injury in fact when telecommunications providers record their phone calls with incarcerated clients. For example, under the Model Rules of Professional Conduct, an attorney is required to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."[59] Thus, an attorney may reasonably decide to cease communicating with a client over a prison phone system, opting exclusively for in-person visits where the attorney can personally guarantee that their conversations will remain private and confidential. As the Western District of Texas noted in the *Austin Lawyers Guild* litigation, "being forced to conduct in-person visits, rather than quick and inexpensive telephone calls demonstrates concrete injury."[60] The court went on to say that, even if attorneys had not suffered this injury, it appeared that the injury was imminent given that the defendants were continuing to "indirectly prevent telephone communications between attorneys and their detained clients."[61] The court recognized an injury in fact even though the attorney–client privilege is a right vested in the client, and the class of plaintiffs in this case was made up exclusively of criminal defense attorneys.[62]

The injury that attorneys are suffering, or could imminently suffer, related to how they communicate with their clients should be held to satisfy the injury requirement for standing in federal court. It thus appears that both prisoner and attorney plaintiffs alike have strong standing arguments in cases against telecommunications providers. Who then is the best litigant for this kind of action?

While it seems that both prisoners and their attorneys satisfy standing, the Prison Litigation Reform Act (PLRA) poses a substantial barrier for current inmates who may wish to bring these claims. The most significant

---

[58] Lory A. Barsdate, Note, *Attorney-Client Privilege for the Government Entity*, 97 YALE L.J. 1725, 1725 n.2 (1988) (citing 8 J. WIGMORE, EVIDENCE IN TRIALS AT COMMON LAW § 2290, at 542 (J. McNaughton rev. ed. 1961)).

[59] MODEL RULES OF PRO. CONDUCT r. 1.6(c) (AM. BAR ASS'N 2020).

[60] Austin Laws. Guild v. Securus Techs, Inc., No. 1:14-CV-366-LY, 2015 WL 10818584, at *4 (W.D. Tex. 2015) (citing Ctr. Hill Def. Fund v. U.S. Army Corps of Eng'rs, Nashville Dist., 886 F. Supp. 1389, 1397 n.5 (M.D. Tenn. 1995) (being forced to drive longer distance to launch boat is concrete injury for standing purposes)); *see also* Caitlin Thistle, Comment, *A First Amendment Breach: The National Security Agency's Electronic Surveillance Program*, 38 SETON HALL L. REV. 1197, 1217 (2008) (arguing attorneys suffer a concrete harm when they are unable to communicate with clients based on fear that communications will be intercepted, breaching attorney–client privilege).

[61] *Austin Laws. Guild*, 2015 WL 10818584, at *4.

[62] *Id.* at *10–*11.

impediment posed by the PLRA is its provision that prevents prisoners from bringing a civil action for compensatory damages for "mental or emotional injury suffered while in custody without a prior showing of physical injury or the commission of a sexual act."[63] Courts have interpreted "mental or emotional injury" broadly to encompass virtually every kind of injury *other* than a physical injury.[64] Thus, in a class of plaintiffs which includes current inmates, the PLRA would effectively bar any Federal Wiretap Act claims for compensatory damages, only allowing plaintiffs to sue for injunctive relief and punitive damages.[65]

Further, the PLRA requires "a prisoner confined in any jail, prison, or other correctional facility" to exhaust all administrative remedies available to him before being able to bring suit under any federal law.[66] Based on this statutory provision, a prisoner would likely have to make a showing that he proceeded through all of the administrative procedures available before proceeding with a suit against a telecommunications provider under the Federal Wiretap Act. The PLRA defines "prisoner" broadly as "any person subject to incarceration, detention, or admission to any facility who is accused of, convicted of, sentenced for, or adjudicated delinquent for, violations of criminal law or the terms and conditions of parole, probation, pretrial release, or diversionary program."[67] This broad definition would preclude any person who has yet to be convicted and is awaiting trial in a jail from bringing suit without first exhausting all available administrative remedies. The barriers the PLRA presents provide a plausible, if not probable, explanation for why many of these lawsuits have included either only attorneys, or attorneys and former prisoners.

Accordingly, the best class of plaintiffs in this kind of litigation is a group of criminal defense attorneys supplemented with at least some former

---

[63] 42 U.S.C. § 1997e(e).

[64] *See, e.g.*, Al-Amin v. Smith, 637 F.3d 1192, 1197 n.5, 1199 (11th Cir. 2011) (holding that a plaintiff alleging a violation of the attorney–client privilege had "failed to meet § 1997e(e)'s physical injury requirement."), *rev'd on other grounds*, 993 F.3d 1353 (11th Cir. 2021); Thompson v. Carter, 284 F.3d 411, 418 (2d Cir. 2002) (noting that the "majority position" among the circuits is to require plaintiffs to prove physical injury for recovery of compensatory damages but not for recovery of nominal or punitive damages).

[65] While the PLRA generally requires a showing of physical injury for prisoner plaintiffs to recover compensatory damages, it has become accepted that such a showing is not required to bring a claim for punitive damages. The Eleventh Circuit became the final circuit court of appeals to recognize this distinction in 2021. *See* Hoever v. Marks, 993 F.3d 1353, 1355–56 (11th Cir. 2021) ("Our circuit stands alone in enforcing § 1997e(e) as a complete bar to punitive damages . . . in the absence of physical injury . . . . We now recognize that § 1997e(e) permits claims for punitive damages without a showing of physical injury.").

[66] 42 U.S.C. § 1997e(a).

[67] 18 U.S.C. § 3626(g)(3).

prisoners. This class makes use of all available standing arguments and avoids any PLRA issues affecting current inmates.[68] It would also permit the class to recover both monetary damages and injunctive relief. From a redressability perspective, former prisoners could recover damages for breach of the attorney–client privilege while "enjoining [a telecommunications provider] from recording confidential telephone calls [would] redress the injury alleged" for attorneys who continue to work with incarcerated clients where the improper recordings are taking place.[69] Having addressed standing and outlined the ideal class of plaintiffs for these cases, the next Part analyzes how the substantive provisions of the Federal Wiretap Act from Part I apply to cases against prison telecommunications providers.

III. THE FEDERAL WIRETAP ACT AS A TOOL FOR PRISON WIRETAPPING CASES

While there are nuances to each attorney and prisoner lawsuit against a telecommunications provider, the paradigmatic case can be synthesized into a broadly applicable set of core facts. In nearly every case, the prisoner and attorney litigants allege that, although it is the provider's express policy to not record prisoner–attorney calls, and although the provider and the detention centers it contracts with lead parties to believe prisoner–attorney calls are not recorded, the provider records the calls anyway.[70] The plaintiffs claim that either they did submit their attorneys' phone numbers to the prison for screening and the calls were still recorded,[71] or that the prison did not inform them of the proper procedures to ensure that prisoner phone calls with their attorneys would not be recorded.[72] In every instance, the recorded phone calls come to light and the prisoners and attorneys file suit.[73] In addition to

---

[68] *See* Harris v. Garner, 216 F.3d 970, 979–80 (11th Cir. 2000) ("Because section 1997e(e) applies only to claims filed while an inmate is confined, it does not prevent a former prisoner from filing after release a monetary damages claim for mental and emotional injury suffered while confined, without a prior showing of physical injury.").

[69] Austin Laws. Guild v. Securus Techs., Inc., No. 1:14-CV-366-LY, 2015 WL 10818584 at *5 (W.D. Tex. Feb. 4, 2015).

[70] *See* Plaintiffs' Response to Defendant's Renewed Motion to Dismiss at 1–2, Austin Laws. Guild v. Securus Techs., Inc., No. 1:14-cv-00366-LY, 2014 WL 6471539 (W.D. Tex. Sept. 5, 2014); Pratt v. Securus Techs., Inc., No. 1:20-cv-00295-JDL, 2021 WL 1725936 at *2 (D. Me. Apr. 30, 2021).

[71] Romero v. Securus Techs., Inc., 331 F.R.D. 391, 399 (S.D. Cal. 2018); Johnson v. CoreCivic, No. 4:16-cv-00947-SRB, 2018 WL 7918162 at *1 (W.D. Miss. Sept. 18, 2018).

[72] Plaintiffs' Response to Defendant's Renewed Motion to Dismiss, *supra* note 70, at 1–2; *Pratt*, 2021 WL 1725936 at *2.

[73] While this Note focuses on the Federal Wiretap Act, plaintiffs in these cases often bring additional causes of action, most notably violations of analogous state laws. *See, e.g.*, First Amended Class Action Complaint paras. 81–92, Bliss v. CoreCivic, Inc., No. 2:18-cv-01280-JAD-GWF, 2018 WL 7982129 (D. Nev. Sep. 28, 2018) (bringing a Nevada Wiretap Claim in additional to Federal Wiretap Act claim). Other lawsuits go further still, alleging various state law violations including, among other things, fraud and

lack of standing, the most common defenses against these claims are those outlined in Part I: lack of intent, consent, and the business-extension exception. This Part will address and rebut each of those arguments.

A. Analyzing Intent

Based on other recent cases and on the Federal Wiretap Act landscape broadly, it seems that litigants have a realistic chance of ultimately proving intent if they can show that a provider was on notice that its system was routinely recording attorney–client communications at a specific facility or a specific set of facilities, and failed to take remedial measures to correct the problem. In 1986, Congress dropped the word "willfully" from § 2511 of the Federal Wiretap Act and replaced it with "intentionally."[74] This meant that defendants in Federal Wiretap Act cases no longer needed to *know* that they were violating a legal duty to be found liable.[75] Plaintiffs now only have to prove that a defendant intended to intercept the communication in a prohibited fashion. However, the change only lowered the bar slightly, making it so that the "ignorance of the law" defense would not apply to Federal Wiretap Act claims.[76] Plaintiffs still must show that the defendant's conduct was intentional—as opposed to accidental.

The difficulty with this standard is that it requires a plaintiff to get into the defendant's head.[77] If defendants can simply claim mistake or negligence, then they can effectively shield themselves from liability under the Federal Wiretap Act. But like many other forms of criminal and civil intent, courts have developed ways in which plaintiffs can establish the existence of intent based on "ample circumstantial evidence."[78] Several federal courts across the country have relied on circumstantial evidence to justify findings of intent.[79]

---

intentional misrepresentation on the basis that Securus leads prisoners to believe their calls with their attorneys will not be recorded, but proceeds to record them anyways. *See* Second Amended Complaint paras. 141–69, Romero v. Securus Techs., Inc., 331 F.R.D. 391 (S.D. Cal. 2018).

[74] Karnezis, *supra* note 24, § 2(a).

[75] *See, e.g.*, Earley v. Smoot, 846 F. Supp. 451, 453 (D. Md. 1994) (finding that, when Congress dropped the willfulness requirement from the Federal Wiretap Act, it clearly made it true that "liability may be imposed under § 2511(1)(a) merely for intentional—in the traditional sense of purposeful—conduct, without a showing of disregard of a known legal duty").

[76] *See* Peavy v. WFAA-TV, Inc., 221 F.3d 158, 178 (5th Cir. 2000).

[77] *See* Roy D. Gross, *Can an Inference of Intent to Induce Infringement of a Patent Be Drawn Where Other Reasonable Inferences Exist? An Examination of the Use of Circumstantial Evidence to Prove Inducement of Infringement*, 14 MINN. J.L. SCI. & TECH. 765, 767–68 (2013) (discussing how "when circumstantial evidence is used" it can be difficult to prove specific intent because "the circumstantial evidence must be used to draw an inference to the [opposing party's] state of mind").

[78] *See* Abraham v. Cnty. of Greenville, 237 F.3d 386, 392 (4th Cir. 2001).

[79] *See In re* Google Assistant Priv. Litig., 457 F. Supp. 3d 797, 815 (N.D. Cal. 2020) ("interceptions may be considered intentional where a defendant is aware of the defect causing interception and takes no remedial action"); Backhaut v. Apple, Inc., 74 F. Supp. 3d 1033, 1044 (N.D. Cal. 2014) (finding

Establishing intent in this way under the Federal Wiretap Act boils down to showing that the defendant was aware of a defect which caused the improper interception of calls and that the defendant failed to take any remedial measures to fix the problem.[80]

Circumstantial evidence of intent has appeared in several Federal Wiretap Act complaints in the prisoner–attorney phone call context, with varying degrees of success. For example, the District of Nevada in *Bliss* found intent on the part of the defendant, CoreCivic,[81] in denying its motion to dismiss. There, the plaintiffs claimed that there were numerous other lawsuits across the country based on similar facts, that CoreCivic had admitted there was no legitimate need to record calls between prisoners and attorneys in other litigation, and that CoreCivic was under cease-and-desist orders in Kansas for the same sort of conduct.[82] The plaintiffs alleged that these facts all supported a finding of intentionality, particularly at the pleading phase. The court agreed, finding that "Bliss's allegations [were] more than enough to plead intentionality," especially because intent under the Federal Wiretap Act is met if the interception is done on purpose, "even if that purpose was not nefarious and the actor was unaware that the use was unlawful."[83]

On the other end of the spectrum, the District of Maine has been far more reluctant to infer intent, even on a motion to dismiss, based on similar circumstantial evidence. The plaintiffs in *Pratt* argued in their most recent complaint that defendant "Securus's knowledge [could] be inferred from two

complaint survived motion to dismiss on basis of intent because plaintiffs alleged defendant was aware of a defect and made the conscious decision not to fix it); Anderson v. City of Columbus, 374 F. Supp. 2d 1240, 1247 (M.D. Ga. 2005) ("[E]vidence exists that [the defendant] was aware of the glitch in the recording system when the headsets were used. Therefore, a reasonable jury could conclude that [the defendant] knew that the system would record Plaintiff, and she intentionally failed to tell Plaintiff how to prevent the recording."); Narducci v. Vill. of Bellwood, 444 F. Supp. 2d 924, 935 (N.D. Ill. 2006) ("It is enough to be aware that such interception is occurring and to fail to stop it.").

[80] *See In re* Google Assistant Priv. Litig., 457 F. Supp. 3d at 815. In the prison context, this standard of intent is analogous to the subjective, "deliberate indifference" standard applied to Eighth Amendment claims surrounding inadequate medical care. *See* Estelle v. Gamble, 429 U.S. 97, 106 (1976) ("In order to state a cognizable claim, a prisoner must allege acts or omissions sufficiently harmful to evidence deliberate indifference to serious medical needs.").

[81] CoreCivic is the largest private owner of "correctional, detention and residential reentry facilities" in the United States. *About Us*, CORECIVIC, https://www.corecivic.com/about [https://perma.cc/4SZB-YS3N]. In *Bliss*, CoreCivic, the private prison company, did not contract with a separate telecommunications firm but instead operated their own phone system within the detention facilities at issue in the litigation. *See* Bliss v. CoreCivic, Inc., 580 F. Supp. 3d 924, 926 (D. Nev. 2022). As mentioned earlier in this Note, the exact defendant in these cases is immaterial to the analysis, and the allegations against CoreCivic in *Bliss* are nearly identical to those plaintiffs make against an outside telecommunications provider.

[82] *Bliss,* 580 F. Supp. 3d. at 929.

[83] *Id.*

factual allegations."[84] First, Securus had been "sued four times in other jurisdictions for allegedly unlawfully recording attorney-client calls."[85] And second, Securus "recorded 'over 800' attorney-client calls in Maine since July 2019, [encompassing] 'over 150 inmates.'"[86] However, for the second time in the last year, the court dismissed the complaint for failing to plausibly allege that Securus "intentionally recorded attorney-client calls."[87] The court reasoned that the previous allegations against Securus were unpersuasive because none of the four lawsuits that the plaintiffs relied upon resulted in a judicial finding or judgment and thus did not support an inference that Securus was on notice that what they were doing was unlawful.[88] Concerning the sheer number of the calls, the court pointed out that the complaint "provide[d] a numerator without a denominator and d[id] not indicate whether the recordings represented a minor glitch or a systemic problem."[89]

The court's analysis in *Pratt* is problematic for several reasons. First, and perhaps most striking, is the fact that the court decided the issue on a motion to dismiss.[90] In deciding a motion to dismiss, the court must assume the factual allegations are true and consider them in the light most favorable to the nonmoving party.[91] The facts that the plaintiffs in *Pratt* alleged in their complaint do support an inference that Securus acted intentionally, especially at the motion to dismiss stage. And taking the plaintiffs' factual allegations as true further defeats the specific arguments offered by the court in dismissing the *Pratt* case.

First, as to the probative value of the other lawsuits to which the plaintiffs alluded, the court failed to properly evaluate the notice that such suits could provide to Securus. It may be true that the mere existence of other lawsuits does not go far enough to establish an ultimate finding of intent given that there have been no judicial findings in those cases. However, the existence of several lawsuits alone substantially corroborates the notion that

---

[84] Pratt v. Securus Techs., Inc., No. 1:20-cv-00295-JDL, 2021 WL 5094907, at *4 (D. Me. Nov. 2, 2021).

[85] *Id.*

[86] *Id.*

[87] *Id.* at *5; *see Pratt* v. Securus Techs., Inc., No. 1:20-cv-00295-JDL, 2021 WL 1725936, at *6 (D. Me. Apr. 30, 2021).

[88] *Pratt*, 2021 WL 5094907, at *4.

[89] *Id.* at *5.

[90] Motions to dismiss are raised early in the litigation process, and judges decide them based purely on what is included in the plaintiff's complaint. The standard for surviving a motion to dismiss is not particularly high. All that is required is "a short and plain statement of the claim showing that the pleader is entitled to relief," such that the defendant has "fair notice" of the claim or claims being brought against them. Fed. R. Civ. P. (8)(a)(2); Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555 (2007).

[91] *See Twombly*, 550 U.S. at 555; Manzarek v. St. Paul Fire & Marine Ins. Co., 519 F.3d 1025, 1031 (9th Cir. 2008).

Securus knew of potential shortcomings in its technology and that those problems have persisted for many years. Moreover, other lawsuits demonstrate additional evidence of system-wide failures, which goes directly to the question of whether Securus was aware of a defect and failed to take any remedial measures.

Second, as to the notion that the plaintiffs failed to contextualize the number of recorded calls and demonstrate whether those recordings were representative of a glitch or a broader problem, if the court had considered this allegation in the plaintiffs' favor, it would have assumed that it was a systematic problem like the court in *In re Google Assistant Privacy Litigation*. Deciding a motion to dismiss, the court in the *Google* litigation found that "some *de minimis* error rate . . . may be tolerated without expos[ure] . . . to liability" but that, at the motion to dismiss stage, the court would not assume that the rate of improper interceptions was *de minimis*.[92] Furthermore, it is unclear how the plaintiffs in *Pratt* could provide the denominator of total attorney calls without the opportunity to move forward with discovery.

The court's decision in *Pratt* also barred the plaintiffs from having any opportunity to collect additional evidence of Securus's intent through discovery. Discovery often proves crucial for uncovering additional evidence of intent. For example, in a Federal Wiretap Act case that went to trial in the District of South Carolina, intent was "vigorously disputed."[93] Ultimately the jury returned a verdict against the defendant, the County of Greenville, for setting up a comprehensive recording system in a local detention center that ended up intercepting phone calls made from the judicial corridor of the center, a separate section in the center with "offices and courtroom facilities for city and county judges."[94] The Fourth Circuit affirmed the decision, finding that there was ample circumstantial evidence presented at trial to support a finding of intent, in part based on a confidential memorandum that came out at trial indicating that county officials were aware of the judicial corridor recordings but failed to rectify the issue.[95] A confidential memorandum is a quintessential example of circumstantial evidence that a plaintiff cannot be expected to have and rely on in the pleading stage. Based on the strength of the facts alleged in the plaintiffs' complaint in *Pratt* and the importance of discovery in further establishing intent, the court should have denied Securus's motion to dismiss.

---

[92] *See In re* Google Assistant Priv. Litig., 457 F. Supp. 3d 797, 815–16 (N.D. Cal. 2020).

[93] Abraham v. Cnty. of Greenville, 237 F.3d 386, 388 (4th Cir. 2001).

[94] *Id.* at 388–89.

[95] *Id.* at 392–93.

That said, the court's ruling in *Pratt* helpfully illustrates how courts may think about intent beyond the pleading phase—and in particular, the emphasis they place on notice. In other words, plaintiffs will likely have to show something beyond an uncontextualized number of recorded calls or the existence of litigation in other districts to survive summary judgment motions and ultimately prevail at trial. The *Huff* and *Austin Lawyers Guild* cases demonstrate this point.[96] These cases repeatedly put Securus on notice about their conduct and how their system intercepted privileged communications. In *Huff*, the plaintiffs alleged that Securus was aware "they were operating a system that captured and recorded confidential attorney-client communications."[97] Notably, the plaintiffs in *Huff* had the benefit of relying on a 2016 cease-and-desist order where the same district court demanded Securus stop recording attorney–client communications in a detention center in Leavenworth, Kansas.[98] Securus's continued recording at Leavenworth following the order is what gave rise to the *Huff* litigation.[99] *Huff* ultimately settled before trial.[100]

The idea of notice may, understandably, give plaintiffs some pause. Claimants might reasonably prefer to take a case directly to court instead of putting the provider on notice, thus giving it an opportunity to rectify the problem before taking legal action. However, putting a provider on notice can support a finding that the defendant was aware that its technology and processes were deficient when it comes to intercepting attorney–client communications. This, in turn, supports a finding of intent, especially if other facts give rise to a reasonable assumption that a provider's technology is substantially similar in all of the facilities with which it contracts. Nevertheless, especially given the court's skepticism in *Pratt*, plaintiffs will likely need more. Substantial pretrial investigation—both through discovery and otherwise—will likely prove necessary to form a cohesive and persuasive argument that a telecommunications provider was aware of a problem with its recording system. Plaintiffs should seek evidence of any

---

[96] *See* Huff v. CoreCivic, Inc., No. 17-2320-JAR-JPO, 2018 WL 1175042 (D. Kan. Mar. 5, 2018); Austin Laws. Guild v. Securus Techs., Inc., 2015 WL 11237655 (W.D. Tex. Mar. 23, 2014).

[97] Complaint para. 21, *Huff*, 2018 WL 1175042.

[98] *See* United States v. Black, 2017 WL 2151861 at *2 (D. Kan. May 17, 2017).

[99] *See* Huff v. CoreCivic, Inc., No. 2:17-cv-02320-JAR-JPO, 2020 WL 430212, at *1 (D. Kan. Jan. 28, 2018) ("Plaintiffs allege that after entry of this Court's 2016 cease and desist order in *United States v. Black* . . . Defendants continued to record attorney-client telephone calls for no legitimate reason . . . ."). Although Securus moved to dismiss the plaintiff's Federal Wiretap Act claim in *Huff*, it did not argue that the plaintiffs failed to plausibly allege intent. *See* Memorandum in Support of Defendant Securus's Motion to Dismiss Plaintiffs' Complaint, Huff v. CoreCivic, Inc., No. 17-2320-JAR-JPO, 2018 WL 1175042 (D. Kan. Mar. 5, 2018) (arguing the business-extension exception alone served as the basis for why the court should dismiss).

[100] Margolies, *supra* note 12.

communications establishing that the provider knew the detention facilities were doing an insufficient job of screening out attorney–client calls, public records that might help establish the total scale of the problem in the facility in question, and similarities with the recording systems in other districts where litigation has called into question the system's functionality.

If a provider becomes aware that its system is routinely intercepting calls between attorneys and their prisoner clients and fails to do anything to rectify the issue, then continued use of the recording system will inevitably lead to the recording of more privileged calls. Once a provider is on notice, it can no longer claim mistake, accident, negligence, or even recklessness. Under the Federal Wiretap Act, knowing a risk exists and staying the course amounts to more than recklessness—courts should find intent on these facts. Notice to a provider ahead of litigation and a subsequent failure on behalf of the company to make any changes—combined with "ample circumstantial evidence"—provides an adequate basis for proving intent.[101]

B. Analyzing Consent

Plaintiffs who can establish that a telecommunications provider intentionally intercepted their privileged communications will also need to rebut arguments that the provider's conduct falls into an exception to the Federal Wiretap Act. The first relevant exception is consent. Consent is a fact-intensive inquiry which frequently hinges on notice and reasonable expectations, both of which are complicated in the prison context where automated messages are the norm.

Most recorded prison phone calls fall under the Federal Wiretap Act's consent exception.[102] At the beginning of most calls, there is a recorded message stating something along the lines of, "this call is from a correctional facility and may be monitored and recorded."[103] Prisoners, and the people with whom they speak, who hear this message and continue the call thus impliedly consent to the recording of the conversation. For example, in *Faulkner*, an inmate received an orientation manual when he arrived at the prison that stated "[t]elephones are subject to recording and monitoring."[104] Inmates at the prison were also notified during an orientation that their calls may be subject to recording, signs were posted over each of the prison's telephones indicating that calls were subject to monitoring, and an automated message played at the beginning of calls notifying users of possible

[101] Abraham v. Cnty. of Greenville, 237 F.3d 386, 392 (4th Cir. 2001).

[102] 18 U.S.C. § 2511(2)(d); *see infra* note 103 and accompanying text.

[103] Smith & Lee, *supra* note 1.

[104] United States v. Faulkner, 439 F.3d 1221, 1222 (10th Cir. 2006).

recording.[105] Based on this notice, the Tenth Circuit rejected the plaintiff's argument that there was an inadequate showing of consent to justify the recording. Even though the prisoner who received the notice was not a party to the litigation, the court found that the exception still applied "because the consent of one party is enough."[106] When prisoners are given explicit notice that their communications will be recorded and they make the decision to use their correctional facility's phone system anyway, courts will find that such action is sufficient to support a finding of implied consent for a claim brought under the Federal Wiretap Act.

However, this analysis stops short of completely shielding a provider from liability under the Federal Wiretap Act for recording prisoner phone calls with their attorneys. In *Campiti*, the Massachusetts Commissioner of Corrections—an investigator for the Massachusetts Department of Corrections—and two high-ranking prison officials decided to monitor a call between two prisoners housed at different facilities and a sheriff in charge of the House of Corrections.[107] The officials ultimately prepared a report on the call and disclosed it to various individuals, including the Attorney General of Massachusetts.[108] Ultimately, the district court ruled that none of the participants in the call consented to it being monitored, and the First Circuit affirmed the lower court's ruling.[109] The First Circuit noted that no one informed the prisoners that the call would be monitored, and no regulation was in effect that informed the inmates of the possibility that their call would be recorded.[110] The First Circuit stated the argument on consent "boil[ed] down to the proposition that [the plaintiff prisoner] should have known his call would probably be monitored and [], therefore, gave consent."[111] Ultimately, the court found there was no consent, and the prisoner plaintiffs were permitted to recover damages for the defendants' violations of the Federal Wiretap Act. Thus, a lack of notice implies a lack of consent.

Though telecommunications providers generally have automated messages at the beginning of a prisoner phone call, many of these messages explicitly state that attorney calls are not subject to such recording. Further, providers' official policies often exclude attorney calls from recording.[112] If a prisoner hears one of these recordings just before getting on the phone with

---

[105] *Id*. at 1222–23.

[106] *Id*. at 1225.

[107] Campiti v. Walonis, 611 F.2d 387, 389–90 (1st Cir. 1979).

[108] *Id.* at 390.

[109] *Id.* at 394.

[110] *Id.* at 390

[111] *Id.* at 393.

[112] Securus, for example, has a policy that "all calls, except to [the detainee's] Attorney of Record, are subject to monitoring and recording." *Rules and Regulations*, *supra* note 11.

his or her lawyer, there is no contradiction between the official policy and what an inmate has personal knowledge of based on the recording. In other words, a recording that states calls from an attorney of record are exempt from recording is directly in line with the official policy. Thus, there is sufficient information upon which prisoners and their attorneys can base a reasonable expectation of confidential communication, much like the reasonable expectation the court identified in *Campiti*.[113]

But what about a situation in which there is a more generalized prerecording? If a prisoner knows that Securus's policy is to screen out attorney calls, but the recording at the beginning of a call says nothing to that effect, merely stating that "all calls may be subject to recording," the prisoner faces a contradiction between the policy and what he hears before the call with his attorney. In this situation, if a prisoner proceeds with the call, is it at his own risk? More precisely, does this rise to the level of implicit consent that subjects the call to permissible recording?

Based on First and Ninth Circuit case law, it appears that such situations give rise to findings of implied consent such that plaintiffs would not prevail in Federal Wiretap Act cases, despite the apparent contradictions.[114] In *Novak*, there was a contradiction between "an automated message [that] is played at the beginning of every call that is not screened, which warns the inmate that the call is subject to monitoring and recording" and "Massachusetts and the Federal government . . . regulations prohibiting prison officials from monitoring phone calls between inmates and their attorneys."[115] The First Circuit found that the fact a call was between an inmate and an attorney was not instructive for an analysis of implied consent.[116] The court determined that the prisoner caller was on notice that his calls were subject to recording based in large part on the prerecorded message he heard at the beginning of each call.[117] The inmate made no effort to protect the confidentiality of his calls with his attorney, and the court held that he had consented to the calls being recorded, even though there was "no question" that the recordings violated Massachusetts law.[118]

The Ninth Circuit in *Medina* followed the *Novak* court's lead one year later, affirming the district court's finding that implied consent existed when the prisoner heard a generalized warning that calls "may" be recorded but

---

[113] *See Campiti*, 611 F.2d at 393.

[114] *See* United States v. Novak, 531 F.3d 99, 103 (1st Cir. 2008); Medina v. Cnty. of Riverside, No. 07–56540, 2009 WL 118968, at *2 (9th Cir. Jan. 13, 2009).

[115] *Novak*, 531 F.3d at 100.

[116] *Id.* at 103.

[117] *See id.* at 102–03.

[118] *Id*.

proceeded with attorney calls nonetheless, assuming the call would be screened out.[119] Importantly, the district court noted that "[s]omeone who is told that his telephone conversation 'may' be recorded, but who nonetheless places his call, cannot be heard to complain if his call is in fact recorded" and that "[t]he fact that an attorney was involved does not change the analysis under the Act."[120]

Although frustrating, these holdings do seem to allow for two scenarios in which prisoner plaintiffs can successfully argue they did *not* consent to a recording of their attorney calls. First, if the callers did not hear any automated warning at the beginning of a call but the call was still recorded, they can argue that they were not on notice of the recording and thus did not consent. Second, if the callers heard an automated message that explicitly stated all calls, *except for those made to an attorney*, are subject to recording, plaintiffs can argue that this served as confirmation of their assumption that, consistent with a provider's express policies, the company would not record their attorney calls. However, there is a third scenario, in which there is a contradiction between Securus's policies and the automated recording a caller heard. Based on the courts' holdings in *Novak* and *Medina*, if a caller proceeds with their conversation in this scenario, they would likely be found to have consented to Securus recording the call. Plaintiffs should take care to situate their cases in one of these three scenarios to anticipate Securus's defense and arm themselves with a response.

C. Analyzing the Business-Extension Exception

The final defense that providers often raise in response to Federal Wiretap Act claims is that the company is exempt from liability because of the so-called business-extension exception, housed in § 2510(5)(a) of the Act. To violate the statute, telecommunications providers must intercept communications with an "electronic, mechanical, or other device."[121] However, the statute explicitly excludes "any telephone or telegraph instrument, equipment or facility, or any component thereof . . . being used by a provider of wire or electronic communication service in the ordinary course of its business" from the definition of such devices.[122]

Telecommunications providers—which record nearly all inmate calls under their contracts with correctional facilities—often argue that they are simply operating their systems in the regular course of business. Indeed—in

---

[119] *See* Medina v. Cnty. of Riverside, No. CV 06-4144 ABC (Ex), 2007 WL 9717337, at *7 (C.D. Cal. Sept. 26, 2007); *Medina*, 2009 WL 118968, at *2.

[120] *Medina*, 2007 WL 9717337, at *6–7.

[121] 18 U.S.C. § 2510(5).

[122] 18 U.S.C. § 2510(5)(a).

addition to the Federal Wiretap Act's statutory language—the Supreme Court held in *Lanza* that jails are not generally constitutionally protected areas for purposes of Fourth Amendment protections against unwitting recordings and that "[i]n prison, official surveillance has traditionally been the order of the day."[123] This precedent indicates that all recording within a jail or prison happens in the ordinary course of the telecommunications provider's business. However, the *Lanza* Court went on to say that "even in a jail, or perhaps especially there, the relationships which the law has endowed with particularized confidentiality must continue to receive *unceasing protection*."[124] The attorney–client privilege is perhaps the most obvious relationship that the law treats with particularized confidentiality, especially when the conversation involves someone who is either awaiting trial or has been convicted of a crime.

The *Lanza* distinction between general recordings and recordings of confidential communications is critical for an analysis of the business-extension exception as applied to the prisoner–attorney phone call context. This is because a provider would be hard-pressed to identify a justifiable reason for recording conversations between a prisoner and his lawyer, especially given the heightened legal protections over those communications.[125]

In responding to claims that the business-extension exception applies to a company's recording of attorney–client calls, courts have homed in on these protections. They have done so even though the plain language of the business-extension exception seems to place all *equipment* used in the regular course of business outside of the reach of the statute. Under an equipment-focused reading of the exception, courts could deem proper all recordings collected with equipment "being used . . . in the ordinary course of its business."[126]

Thankfully, judges have refused to expand the exception this far, likely for fear that it would make it too easy to escape liability for conduct that otherwise clearly violates the statute. Instead, courts have focused on how a provider *uses* its equipment in different circumstances. For example, in the *Austin Lawyers Guild* litigation, a magistrate judge's report and findings in response to the defense's motion to dismiss indicated that, when Securus records attorney–client calls made from a correctional facility, the company

---

[123] Lanza v. New York, 370 U.S. 139, 143 (1962) (denying petitioner's claim that officials of the State of New York violated his Fourth Amendment rights when they electronically intercepted and recorded conversations between the prisoner and his brother that took place inside a New York jail).

[124] *Id.* at 143–44 (emphasis added).

[125] *See supra* notes 48–50 and accompanying text.

[126] 18 U.S.C. § 2510(5)(a).

could not use the business-extension exception as a shield against liability under the Federal Wiretap Act.[127] The court noted that Securus has an explicit policy against recording attorney–client calls and that recordings are conducted without notice to the prisoners. Ultimately, the court concluded that the plaintiffs sufficiently "alleged recording confidential attorney–client telephone conversations is not within [Securus's] ordinary course of business, necessary to Securus'[s] service."[128]

In pointing to the contradiction between a provider's conduct and their express policies—combined with the heightened legal protections of attorney–client communications—plaintiffs can forcefully counter the argument that recording attorney–client calls is permitted under the business-extension exception.

Based on the strong responses plaintiffs can make to a provider's most common defenses to Federal Wiretap Act liability (lack of intent, consent, and the business-extension exception), federal district court judges should deny a defendant's motions to dismiss and allow these cases to proceed through discovery and, if necessary, to trial.

CONCLUSION

As the Supreme Court has pointed out, although the expectation of privacy in prison may be diminished, "even in a jail, or perhaps especially there, the relationships which the law has endowed with particularized confidentiality must continue to receive *unceasing protection*."[129] The mere fact that someone is incarcerated does not mean they forfeit the critical protection the attorney–client privilege provides. Telecommunications providers should have to answer for their nationwide, repetitive interception of thousands of prisoner phone calls with their counsel. The Federal Wiretap Act provides an important tool for prisoners and attorneys seeking injunctions to stop this predatory conduct and damages for the injuries it inflicts.

The biggest barrier to success for Federal Wiretap Act claims stems from the statute's intent requirement. Telecommunications providers will continue to claim that their interceptions of prisoner phone calls with attorneys are the product of mistake, negligence, or recklessness. However,

---

[127] *See* Austin Laws. Guild v. Securus Techs., Inc., No. 1:14-CV-366-LY, 2015 WL 10818584 at *10–11(W.D. Tex. Mar. 23, 2014); *see also* Huff v. CoreCivic, Inc., No. 17-2320-JAR-JPO, 2018 WL 1175042, at *3 (D. Kan. Mar. 5, 2018) ("The business extension exception generally applies where calls are recorded pursuant to a legitimate business purpose and the recorded employees or parties are on notice of the recordings.").

[128] *Austin Laws. Guild*, 2015 WL 10818584, at *11.

[129] *Lanza*, 370 U.S. at 143–44 (emphasis added).

plaintiffs can establish intentional interceptions based on circumstantial evidence. Courts hearing arguments on intent should offer parties an opportunity to litigate their cases fully and build out theories of liability with the help of discovery and other procedural mechanisms. As to the other most common defenses—standing, consent, and the business-extension exception—plaintiffs should continue building on the momentum that the lawsuits to date have created to overcome these defenses, forcing courts to develop a body of common law that future litigants can rely on when crafting their own arguments.

Time will tell whether courts will agree that the Federal Wiretap Act provides an adequate tool to redress the wrongs that telecommunications providers continue to commit. If courts decide it does not, it is incumbent upon Congress to take swift action to provide an alternative framework that makes it easier for plaintiffs to receive favorable judgments on claims related to the pervasive recording of obviously privileged communications. Regardless, the sheer number of prisoner–attorney calls that are continually recorded represents an alarming trend in state and federal prisons that demands increased attention among the legal and legislative communities.