No. 25-1672

UNITED STATES COURT OF APPEALS FOR THE FIRST CIRCUIT

DEBRA GOULART, individually and on behalf of all others similarly situated; MICHAEL GARBITT, individually and on behalf of all others similarly situated,

Plaintiffs-Appellants,

JANE DOE; JOHN DOE; JANET DOE,

Plaintiffs,

v.

CAPE COD HEALTHCARE, INC.,

Defendant-Appellee.

On Appeal from the United States District Court for the District of Massachusetts in Case No. 1:25-cv-10445-RGS, Judge Richard G. Stearns

PARTIALLY ASSENTED TO MOTION OF THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA FOR LEAVE TO FILE AMICUS CURIAE BRIEF IN SUPPORT OF APPELLEE AND AFFIRMANCE

MARK C. FLEMING
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000
Mark.Fleming@wilmerhale.com

December 18, 2025

Attorney for Amicus Curiae

Pursuant to Federal Rule of Appellate Procedure 29, the Chamber of Commerce of the United States of America ("Chamber") respectfully moves for leave to file a brief as amicus curiae in support of Appellee and affirmance. The proposed amicus brief is attached as Exhibit A. Defendant-Appellee has consented to amicus's motion. Plaintiffs-Appellants refused to provide a position on the relief sought in this motion unless amicus provided an advance copy of its brief.[1]

The proposed brief provides a unique perspective informed by the Chamber's extensive membership and experience in the business and healthcare fields. The Chamber is the world's largest business federation, representing approximately 300,000 direct members and indirectly representing the interests of more than three million businesses and professional organizations of every size, in every industry sector, and from every region of the country. Many of the Chamber's members in the healthcare industry and beyond would be potentially affected by Plaintiffs-Appellants' theory of liability in this case.

Given its perspective and deep understanding of the issues involved, the Chamber regularly participates as amicus curiae in cases involving state and federal Wiretap Acts and third-party website analytics tools. *See, e.g.*, *Popa v. Microsoft*

[1] No counsel for a party authored the amicus brief in whole or in part, and no person or entity, aside from amicus curiae, its members, or its counsel, made any monetary contribution intended to fund the preparation or submission of the brief.

Corp., 153 F.4th 784 (9th Cir. 2025) (application of Pennsylvania Wiretap Act to session-replay technology); *Gutierrez v. Converse Inc.*, No. 24-4797, 2025 WL 1895315 (9th Cir. July 9, 2025) (application of California Invasion of Privacy Act to the use of web-based customer service tools); *Vita v. New England Baptist Hosp*., 494 Mass. 824 (2024) (application of Massachusetts's wiretap law to intercepting web-browsing activity); *Facebook, Inc. v. Davis*, No. 20-727 (U.S. 2020) (application of federal Wiretap Act to follow-up web requests).

In this case, the Chamber's participation is particularly relevant because Plaintiffs-Appellants' claims rest on a novel and expansive interpretation of the federal Wiretap Act that, if accepted, could impose significant compliance burdens and litigation risks across multiple industries. The Chamber's brief addresses the broader implications of such an interpretation, including its potential conflict with established privacy frameworks and its impact on the business community at large.

The proposed brief will therefore "contribute in clear and distinct ways" to the Court's analysis. *Prairie Rivers Network v. Dynegy Midwest Generation, LLC*, 976 F.3d 761, 764 (7th Cir. 2020) (granting the Chamber's motion for leave to file); *see also Neonatology Assocs., P.A. v. Commissioner of Internal Revenue*, 293 F.3d 128, 132 (3d Cir. 2002) (Alito, J.) (an amicus brief may assist the Court "by explain[ing] the impact a potential holding might have on an industry or other group" (quotation marks omitted)). "Even when a party is very well represented, an amicus

may provide important assistance to the court." *Neonatology Assocs.*, 293 F.3d at 132; *see also Gallo v. Essex County Sheriff's Department*, No. 1:10-cv-10260-DPW, 2011 WL 1155385, at *6 n.7 (D. Mass. Mar. 24, 2011) (noting that, "[w]hile the motion was ably presented by" defendant's counsel, "the very thoughtful *amicus* submissions were quite helpful in putting the immediate controversy in its larger context"). And here, the Chamber's proposed brief will "explain[] the broader regulatory or commercial context" in which this case arises and "provid[e] practical perspectives on the consequences of potential outcomes." *Prairie Rivers Network*, 976 F.3d at 763. Specifically, the proposed amicus brief provides context regarding the recent surge in Wiretap Act litigation that implicates HIPAA and addresses the particular concerns facing businesses and healthcare organizations that employ digital engagement tools. The brief further examines the balance between privacy protections and the operational needs of businesses in light of the existing legal and statutory frameworks of HIPAA and the Wiretap Act.

Finally, the proposed amicus brief is being filed within one week of the filing of Appellee's brief on December 11, 2025. *See* Fed. R. App. P. 29(a)(6).

For the foregoing reasons, the Chamber respectfully requests that the Court grant leave to file a brief as amicus curiae and accept the proposed amicus brief for filing.

Respectfully submitted,

/s/ Mark C. Fleming

MARK C. FLEMING
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000
Mark.Fleming@wilmerhale.com

Attorney for Amicus Curiae The Chamber of Commerce of the United States of America

December 18, 2025

CERTIFICATE OF SERVICE

I hereby certify that I filed the foregoing with the Clerk of the United States Court of Appeals for the First Circuit via the Court's CM/ECF system, which will send notice of such filing to all registered CM/ECF users this 18th day of December, 2025.

/s/ Mark C. Fleming
MARK C. FLEMING
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000
Mark.Fleming@wilmerhale.com

December 18, 2025

No. 25-1672

UNITED STATES COURT OF APPEALS FOR THE FIRST CIRCUIT

DEBRA GOULART, individually and on behalf of all others similarly situated; MICHAEL GARBITT, individually and on behalf of all others similarly situated,

Plaintiffs-Appellants,

JANE DOE; JOHN DOE; JANET DOE,

Plaintiffs,

v.

CAPE COD HEALTHCARE, INC.,

Defendant-Appellee.

On Appeal from the United States District Court for the District of Massachusetts in Case No. 1:25-cv-10445-RGS, Judge Richard G. Stearns

BRIEF FOR AMICUS CURIAE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA IN SUPPORT OF APPELLEE AND AFFIRMANCE

Of Counsel:

MARIA C. MONAGHAN
MARIEL A. BROOKINS
U.S. CHAMBER LITIGATION CENTER
1615 H Street NW
Washington, DC 20062
(202) 463-5337

MARK C. FLEMING
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000
Mark.Fleming@wilmerhale.com

December 18, 2025

Attorneys for Amicus Curiae

CORPORATE DISCLOSURE STATEMENT

The Chamber of Commerce of the United States of America states that it is a non-profit, tax-exempt organization incorporated in the District of Columbia. The Chamber has no parent corporation, and no publicly held company has 10% or greater ownership in the Chamber.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

LEGISLATIVE MATERIAL

OTHER AUTHORITIES

STATEMENT OF INTEREST OF AMICUS CURIAE[1]

The Chamber of Commerce of the United States of America (the "Chamber") is the world's largest business federation. It represents approximately 300,000 direct members and indirectly represents the interests of more than three million companies and professional organizations of every size, in every industry sector, and from every region of the country. An important function of the Chamber is to represent the interests of its members before Congress, the executive branch, and the courts. To that end, the Chamber regularly files amicus curiae briefs in cases like this one that raise issues of concern to the Nation's business community.

Many of the Chamber's members develop and utilize internet-based customer-service tools to facilitate communication and easily resolve issues that arise in the everyday course of business. The Chamber has a strong interest in this case because plaintiffs across the country have advanced novel legal theories targeting these technologies and seeking judgments that pose existential risks to businesses. The Chamber's members want these beneficial tools to remain available to businesses and consumers without fear of baseless litigation. Consistent with its interest in this case, the Chamber has filed amicus briefs in

[1] No counsel for a party authored this brief in whole or in part, and no person or entity, aside from amicus curiae, its members, or its counsel, made any monetary contribution intended to fund the preparation or submission of this brief.

courts across the country opposing the aggressive use of wiretap statutes and similar laws to attack industry-standard tools and features. *See Doe v. Lawrence General Hospital*, No. 1:25-cv-10081-NMG (D. Mass. 2025), ECF. Nos. 19, 61; *Gutierrez v. Converse, Inc.*, No. 24-4797 (9th Cir. Jan. 22, 2025), ECF. No. 25; *Popa v. Microsoft Corporation*, No. 24-14 (9th Cir. June 21, 2024), ECF No. 42; *Vita v. New England Baptist Hospital*, No. SJC-13542 (Mass. Mar. 13, 2024); *Salazar v. Paramount Global*, No. 23-5748 (6th Cir. Feb. 2, 2024), ECF No. 20; *Salazar v. National Basketball Association*, No. 23-1147 (2d Cir. Dec. 12, 2023), ECF No. 56; *Facebook, Inc. v. Davis*, No. 20-727 (U.S. Dec. 28, 2020).

SUMMARY OF THE ARGUMENT

This Court should affirm the district court's dismissal of Plaintiffs-Appellants' claim under the federal Wiretap Act, 18 U.S.C. §§ 2510-2522, because the claim rests on a misinterpretation of the statute that would have sweeping and harmful consequences for healthcare providers and other businesses. Plaintiffs-Appellants' claim is part of a growing trend of abusive litigation across the country challenging healthcare providers' and other entities' use of widespread and beneficial website analytics and marketing tools—*i.e.*, third-party software—to collect data about how visitors use their websites and to help the providers share information about their services. Use of these tools does not violate the federal Wiretap Act because the Act is a one-party consent statute and visitors' data is not

collected for the purpose of committing a separate crime or tort. *See* 18 U.S.C. § 2511(2)(d). Plaintiffs-Appellants argue that the Act's crime-tort exception applies because the data collection itself allegedly violates the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Massachusetts tort law. But Plaintiffs-Appellants' theory improperly conflates the act of interception by a party to a communication with the alleged criminal or tortious purpose. The Wiretap Act's plain text, legislative history, and relevant precedent make clear that the Act only prohibits party interception if done with intent to commit a separate criminal or tortious act beyond the mere act of interception itself. And as the district court concluded, Plaintiffs-Appellants did not adequately allege a separate unlawful intent. Appx10-11 ("no data was alleged to have been independently used in a crime or tort committed by CCHC").

Beyond improperly rewriting the Wiretap Act, Plaintiffs-Appellants' misinterpretation of the Act would effectively create a private right of action for HIPAA violations, circumventing Congress's deliberate decision to vest HIPAA enforcement authority exclusively in the federal Department of Health and Human Services and state attorneys general. Their theory would undermine HIPAA's carefully balanced regulatory framework, threaten healthcare providers with massive liability (potentially up to $10,000 per website visitor), and lead to inconsistent judicial interpretations of healthcare privacy obligations. A new,

judicially created HIPAA cause of action via the Wiretap Act would impose significant costs on providers, insurers, and technology companies, ultimately driving up healthcare expenses for patients and consumers. Even the mere threat of Wiretap Act liability, which can include both criminal and civil penalties, may coerce businesses into settling meritless claims, diverting resources away from patient care and innovation. Adopting Plaintiffs-Appellants' theory would also penalize the use of beneficial website analytics and marketing tools that healthcare providers and many other businesses rely on to improve user experience and public-health outcomes, even when their use causes no actual harm.

The Court should affirm the district court's dismissal of Plaintiffs-Appellants' Wiretap Act claim.

ARGUMENT

I. UNDER THE FEDERAL WIRETAP ACT, A PARTY CANNOT BE HELD LIABLE FOR INTERCEPTING A COMMUNICATION UNLESS THE PARTY INTENDS TO COMMIT A SEPARATE CRIMINAL OR TORTIOUS ACT BEYOND THE INTERCEPTION ITSELF

The federal Wiretap Act is a one-party consent statute. It explicitly authorizes a party to a communication to intercept the communication, or to consent to another party's interception of the communication, unless the interception is done for the purpose of committing a criminal or tortious act. The Act provides, in relevant part:

> ***It shall not be unlawful*** under this chapter for a person … ***to intercept*** a wire, oral, or electronic communication ***where such person is a party to the communication or where one of the parties to the communication has given prior consent*** … ***unless*** such communication is ***intercepted for the purpose of committing any criminal or tortious act*** in violation of the Constitution or laws of the United States or of any State.

18 U.S.C. § 2511(2)(d) (emphases added). The crime-tort exception plainly distinguishes the "intercept[ion]" from the "criminal or tortious act," identifying the former as being performed "for the purpose of committing" the latter. *Id*.

For this provision to make textual or policy sense, the crime-tort exception must require an intent to commit a *separate* criminal or tortious act beyond the mere act of interception itself. Otherwise, the exception would swallow the Wiretap Act's party-consent rule. It is "one of the most basic interpretive canons[] that a statute should be construed so that effect is given to all its provisions, so that no part will be inoperative or superfluous, void or insignificant." *Rubin v. Islamic Republic of Iran*, 583 U.S. 202, 213 (2018) (quotation marks and brackets omitted); *see also United States v. Menasche*, 348 U.S. 528, 538-539 (1955) ("It is [a court's] duty to give effect, if possible, to every clause and word of a statute." (quotation marks and citations omitted)). Accordingly, for the federal Wiretap Act's crime-tort exception to apply, the interception must be performed for the purpose of committing a distinct wrongful act beyond the interception itself. It is not enough that the interception itself is alleged to constitute a crime or tort.

Rather, "either the 'primary motivation' or a 'determinative factor' in the actor's decision to record [must be] the intent to commit a criminal or tortious act." *United States v. McHugh*, 57 F. Supp. 3d 95, 99-100 (D. Mass. 2014); *see also United States v. Vest*, 639 F. Supp. 899, 904 (D. Mass. 1986) (citing *United States v. Phillips*, 564 F.2d 32, 34 (8th Cir. 1977)). The Complaint fails to plausibly allege this was the case here.

Although the statute's text is clear, the Wiretap Act's legislative history confirms this understanding. The original bill categorically authorized any interception of a communication with the consent of one party. *See* S. Rep. No. 90-1097, 90th Cong., 2d Sess., at 12 (1968).[2] Senator Hart objected that this authorization conceivably allowed a party to intercept a communication for the purpose of breaking the law and injuring others. He feared that parties would use secret recordings for "insidious purposes such as blackmail, stealing business secrets, or other criminal or tortious acts in violation of Federal or State laws." *Id.* at 175. Senator Hart thus proposed adding the crime-tort exception, explaining that it would prohibit intercepting a communication "when the party acts in any way with an intent to injure the other party to the conversation *in any other way*.

[2] The original language read: "It shall not be unlawful under this Chapter for a party to any wire or oral communication, or a person given prior authority by a party to the communication to intercept such communication." S. Rep. No. 90-1097, 90th Cong., 2d Sess., at 12 (1968).

For example, … for the purpose of blackmailing the other party, threatening him, or publicly embarrassing him." 114 Cong. Rec. 14,694-14,695 (1968) (emphasis added).

Circuit courts interpreting the Wiretap Act agree that the crime-tort exception applies only when a party to a communication intercepts it with a specific intent to commit a separate criminal or tortious act beyond the act of interception itself. "[A]ll authority of which we are aware," the Third Circuit declared, "indicates that the criminal or tortious acts contemplated by § 2511(2)(d) are acts secondary to the acquisition of the communication involving tortious or criminal use of the interception's fruits." *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 806 F.3d 125, 145 (3d Cir. 2015).

The Ninth Circuit rejected a claim because the plaintiffs did not allege "that the [interception] tape was made for the purpose of committing some other subsequent crime or tort," but instead "argue[d] that the taping itself was tortious." *Sussman v. American Broad. Cos.*, 186 F.3d 1200, 1202 (9th Cir. 1999); *see also Planned Parenthood Fed'n of Am., Inc. v. Newman,* 51 F.4th 1125, 1135-1136 (9th Cir. 2022) ("A recording has a criminal or tortious purpose under § 2511(1) when 'done for the purpose of facilitating some further impropriety'" (citation omitted)). "Where the taping is legal, but is done for the purpose of facilitating some further impropriety, such as blackmail, [the crime-tort exception] applies." *Sussman*, 186

F.3d at 1202-1203. "Where the purpose is not illegal or tortious, *but the means are*, the victims must seek redress elsewhere." *Id.* (emphasis added).

The Second Circuit likewise held that "[a] cause of action under [the crime-tort exception] requires that the interceptor intend to commit a crime or tort independent of the act of recording itself." *Caro v. Weintraub*, 618 F.3d 94, 100 (2d Cir. 2010). "Had Congress intended for the act of recording itself to provide the tortious intent necessary," the Second Circuit reasoned, "it could have chosen to define the exception in terms of interception of oral communications *resulting* in a tortious or criminal act." *Id.* at 101.

And the Eighth Circuit similarly observed that "the sort of conduct contemplated [by the crime-tort exception] was an interception by a party to a conversation with an intent to use that interception against the non-consenting party in some harmful way and in a manner in which the offending party had no right to proceed." *Meredith v. Gavin*, 446 F.2d 794, 799 (8th Cir. 1971).

II. PLAINTIFFS-APPELLANTS' MISINTERPRETATION OF THE WIRETAP ACT WOULD EFFECTIVELY CREATE A PRIVATE RIGHT OF ACTION FOR HIPAA VIOLATIONS, THWARTING THE CAREFULLY BALANCED STATUTORY ENFORCEMENT SCHEME

Plaintiffs-Appellants' misinterpretation of the Wiretap Act would significantly alter the consequences of alleged HIPAA violations by effectively creating a private right of action, which Congress explicitly declined to include in HIPAA, instead vesting exclusive enforcement authority in the federal Department

of Health and Human Services (HHS) and state attorneys general. 42 U.S.C. § 1320d-5(a)(1), (d)(1). "[I]nterpretations of a statute which would produce absurd results are to be avoided if alternative interpretations consistent with the legislative purpose are available." *Griffin v. Oceanic Contractors, Inc.*, 458 U.S. 564, 575 (1982); *see also Holy Trinity Church v United States*, 143 U.S. 457, 460 (1892) (rejecting statutory reading that would lead to an absurd result). HIPAA's exclusive enforcement regime centralizes authority with HHS to ensure uniformity in privacy and security standards, prevent inconsistent state-level enforcement, and promote compliance through administrative oversight rather than private litigation. Improper expansion of the Wiretap Act would circumvent HIPAA's carefully balanced regulatory framework, threatening covered entities and business associates with significant civil and even criminal penalties. The Wiretap Act's private right of action authorizes statutory damages up to $10,000 per violation, plus potential punitive damages and attorney's fees not available under HIPAA. 18 U.S.C. § 2520(b)(2)-(3), (c)(2)(B). Violators of the Wiretap Act also face up to 5 years in prison and $500,000 in fines. *Id.* §§ 2511(4), 3571.

Plaintiffs-Appellants' theory would increase the already significant costs of providing healthcare. National health care spending was approximately $4.9 trillion or $14,570 per capita in 2023, accounting for 17.6% of the GDP. *National Health Expenditure Data: Historical*, Centers for Medicare & Medicaid Services,

https://www.cms.gov/data-research/statistics-trends-and-reports/national-health-expenditure-data/historical (last updated Dec. 18, 2024).

A substantial portion of healthcare costs is attributable to regulatory compliance. "[T]he costs that hospitals have incurred for implementing HIPAA's privacy provisions," for example, "are estimated to exceed $22 billion." Jack Brill, *Giving HIPAA Enforcement Room to Grow: Why There Should Not (Yet) Be a Private Cause of Action*, 83 Notre Dame L. Rev. 2105, 2132-2133 (2008). "According to one study, the costs associated with implementing HIPAA ranged from a minimum of $10,000 for a small physician group practice[] to as much as $14 million for a larger covered entity." *Id*. To comply with HIPAA's highly technical guidelines, providers must train their staff, employ privacy officers, develop policies, and install special equipment. *Id.* And these costs inevitably are passed on to health care consumers. *Id*. at 2135.

The costs of HIPAA compliance, while significant, are at least somewhat limited and predictable because Congress chose not to provide a private right of action for HIPAA violations. *See Payne v. Taslimi*, 998 F.3d 648, 660 (4th Cir. 2021). Indeed, alleged harms for "privacy violations" are often intangible, while the legal costs to defend against them can be immense. *See* U.S. Chamber of Commerce, Institute for Legal Reform, *Ill-Suited: Private Rights of Action and Privacy Claims*, 1-14 (July 2019), available at https://perma.cc/5JEJ-V7ZV

(detailing how private rights of action, which often allege "intangible[] or nonexistent" harms, "clutter the courts," "chill[] innovation," and increase costs).

Private rights of action are also prone to abuse. Plaintiffs-Appellants' conclusory HIPAA allegations epitomize the type of meritless claims that would proliferate under the complaint's expansive theory of Wiretap Act liability. Plaintiffs-Appellants rely on vague, sweeping assertions untethered to any concrete factual allegations. If accepted, Plaintiffs-Appellants' approach would transform HIPAA into a tool for opportunistic litigation, with no corresponding improvement in protection of patient privacy.

"When representative plaintiffs seek statutory damages, [the] pressure to settle may be heightened because a class action poses the risk of massive liability unmoored to actual injury." *Shady Grove Orthopedic Assocs., P.A. v. Allstate Ins. Co.*, 559 U.S. 393, 445 n.3 (2010) (Ginsburg, J., dissenting). Indeed, pressure to settle even weak or meritless claims can be immense because class-wide statutory penalties for technical violations causing no actual harm to consumers could bankrupt an entire company. *See Stillmock v. Weis Markets, Inc.*, 385 F. App'x 267, 281 (4th Cir. 2010) (Wilkinson, J., concurring).

The Partners Healthcare[3] settlement provides a good example. There, the defendant hospitals paid $18.4 million to settle claims like Plaintiff's once they survived an initial motion to dismiss.[4] Many putative class actions alleging Wiretap Act violations based on use of web analytics software were filed in quick succession following that settlement.[5]

Creating a costly new private cause of action for HIPAA violations through distortion of the Wiretap Act would only exacerbate these issues, thwarting Congress's deliberate decision to foreclose private relief under HIPAA itself. By allowing private plaintiffs to pursue claims under a statute never intended to regulate healthcare privacy, Plaintiffs-Appellants' misinterpretation would further inflate compliance costs, burden the courts with speculative claims, and drive up healthcare expenses for providers and consumers alike.

---

[3] Now known as Mass General Brigham. *See* Mass General Brigham, *Advancing Care*, Mass General Brigham, https://www.massgeneralbrigham.org/en/about/advancing-care (last visited Feb. 19, 2025).

[4] Steve Alder, *Mass General Brigham Settles 'Cookies Without Consent' Lawsuit for $18.4 Million*, HIPAA J. (Jan. 20, 2022), https://www.hipaajournal.com/mass-general-brigham-settles-cookies-without-consent-lawsuit-for-18-4-million/.

[5] *See* Exhibit C to Defendants-Appellants' Application for Direct Appellate Review, *Vita v. New England Baptist Hosp., et al.*, No. DAR-29590 (Mass.) (filed Dec. 1, 2023) (listing known cases alleging Wiretap Act violations as of December 1, 2023).

III. PLAINTIFFS-APPELLANTS' MISINTERPRETATION OF THE WIRETAP ACT THREATENS MANY BUSINESSES WITH SIGNIFICANT LIABILITY FOR USING PREVALENT TECHNOLOGY THAT BENEFITS CONSUMERS

Plaintiffs-Appellants' misinterpretation of the Wiretap Act would expose healthcare providers and many other businesses to potentially crippling liability for using widespread website analytics tools that benefit patients and consumers generally. Businesses use these industry-standard tools to design more user-friendly websites and deliver more relevant advertising. By criminalizing the use of such technology, Plaintiffs-Appellants' distortion of the Wiretap Act's crime-tort exception would harm businesses and consumers alike.

Healthcare providers rely on website analytics tools to better serve patients and to share valuable information about available healthcare services. HIPAA and its implementing regulations seek to "strike a balance between two competing objectives"—"improving the efficiency and effectiveness of the national health care system and preserving individual privacy in personal health information." *Citizens for Health v. Leavitt*, 428 F.3d 167, 171 (3d Cir. 2005); *see also Summary of the HIPAA Privacy Rule*, U.S. Dep't of Health & Hum. Servs, https://perma.cc/MCG3-QFHX ("A major goal of the Privacy Rule is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well-being.").

While carefully safeguarding patient privacy, hospitals, health systems, and other healthcare providers also strive to fulfill the other side of the HIPAA balance by "shar[ing] accurate health information with the public." U.S. Surgeon General Vivek H. Murthy, *Confronting Health Misinformation* (2021), https://perma.cc/YD2V-4QJE. Such information sharing is critical for patients to receive proper care:

> Information is essential fuel for the engine of health care. Physicians, medical professionals, hospitals and other clinical institutions generate, use and share it to provide good care to individuals, to evaluate the quality of care they are providing, and to assure they receive proper payment from health plans. … The capability for relevant players in the health care system – including the patient – to be able to quickly and easily access needed information to make decisions, and to provide the right care at the right time, is fundamental to achieving the goals of health reform.

Understanding Some of HIPAA's Permitted Uses and Disclosures, U.S. Dep't of Health & Hum. Servs., https://perma.cc/N7FC-DTW8.

To facilitate these information-sharing efforts, many hospitals and health systems use third-party technologies, such as the web analytics tools at issue in this case. Website analytics tools lead to more efficient and effective customer experiences by providing insight into whether a website is operating efficiently and effectively. James J. Cappel & Zhenyu Huang, *A Usability Analysis of Company Websites*, 48(1) J. Comput. Info. Sys. 117, 117 (2007) (businesses typically seek "clarity, simplicity, and consistency in web design so that users can perform

desired operations efficiently and effectively. If a website lacks these characteristics, users may become confused or frustrated and 'take their business' to competing sites."). Seemingly recognizing this, HHS does not prohibit the use of such technology on health care provider websites, but "simply cautions providers to be careful how they use such technology so as not to inadvertently disclose private health information." *Doe I v. Google LLC,* 741 F. Supp. 3d 828, 841 (N.D. Cal. 2024).

Hospitals use data gleaned from website analytics tools to improve delivery of healthcare. Such data include information regarding the level and concentrations of community concern regarding medical questions and the areas of a hospital website that people have trouble navigating. Website data analytics can tell a hospital how many website visitors in the past month sought information about, say, RSV vaccines or diabetes treatment in a particular area, which in turn allows hospitals to allocate their resources more effectively.[6] Analytics tools also help hospitals ensure that their public-facing webpages are user-friendly, helping community members more easily find the healthcare information that they need.

Third-party technologies like these, which typically rely on a visitor's IP address to function, enable hospitals and health systems to hone their websites'

[6] Wylie Wong, *How Hospitals Use Analytics to Staff Up Before a Rush*, HealthTech Magazine (Oct. 29, 2019), https://healthtechmagazine.net/article/2019/10/how-hospitals-use-analytics-staff-rush

functionality and the helpfulness of their information. Just as importantly, these technologies allow hospitals and health systems to adjust and publicize information and services in response to public need and thereby improve public health.

Plaintiffs-Appellants' theory of the Wiretap Act also threatens many other businesses outside the healthcare industry. Google Analytics is the "most popular site analytics tool in use."[7] One recent survey estimated that roughly 53% of all websites use Google Analytics; the same survey concluded that the Meta Pixel was used on roughly 11% of all websites, making it the second-most used analytics tool.[8] As discussed above, *see supra* pp. 9-10, under Plaintiff's theory, a business using such analytics tools could face up to $10,000 in statutory damages for every visitor to its website and criminal liability, including prison time, for the business and its employees. 18 U.S.C. §§ 2511(4), 2520(b)(2)-(3), (c)(2)(B), 3571. A business with 5,000 monthly website visits (a number far smaller than for most healthcare systems' websites) could thus face $600 million in damages each year.[9]

---

[7] *See Fraud Detection Through Data Analytics: Identifying Anomalies and Patterns*, Int'l Ass'n of Bus. Analytics Certification (Sept. 20, 2023), https://perma.cc/375C-377T. at 6 n.2 (describing Google Analytics as "the industry standard website analytics platform").

[8] *Usage Statistics and Market Share of Google Analytics for Websites*, W3Techs (Mar. 6, 2024), https://perma.cc/3DYR-767C.

[9] *See* Anna Fitzgerald, *How Many Visitors Should Your Website Get? [Data from 400+ Web Traffic Analysts]*, HubSpot (June 19, 2023), https://perma.cc/3EG8HWBE (showing that three-quarters of small businesses with 11 to 25 employees receive 1,001 to 15,000 monthly visits).

These crushing penalties could force hospitals, healthcare providers, and other companies out of business.

Obtaining website visitors' consent going forward is no solution. When businesses do obtain consent, plaintiffs often challenge the adequacy of the notice a website provides to its users about its use of analytics tools. *See, e.g.*, *Vonbergen v. Liberty Mut. Ins. Co*., 705 F. Supp. 3d 440, 459 (E.D. Pa. 2023) (plaintiff alleging that she "was not presented with any type of pop-up disclosure or consent form"); *Yoon v. Lululemon USA, Inc.,* 549 F. Supp. 3d 1073, 1081 (C.D. Cal. 2021) (plaintiff alleging that she did not consent where the website did not "prompt[] [users] to take any affirmative action to demonstrate assent"). Plaintiffs also often argue that the adequacy of notice and consent cannot be resolved on a motion to dismiss. *See, e.g.*, *Smith v. Google, LLC*, 735 F. Supp. 3d 1188, 1201 (N.D. Cal. 2024) (adopting plaintiff's view that adequacy of consent and notice is a fact dispute that cannot be resolved at motion to dismiss stage).

Thus, even if Wiretap Act claims lack merit, they nevertheless impose substantial litigation costs and exert significant pressure on defendants to settle—which is usually the point, particularly when claims are brought as a putative class action. *See, e.g.*, *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333, 350 (2011) (putative class actions present a significant "risk of 'in terrorem' settlements," because defendants "[f]aced with even a small chance of a devastating loss … will

be pressured into settling questionable claims"). If this Court adopts Plaintiffs-Appellants' interpretation of the crime-tort exception, suits like this—which involve no actual wrongdoing and no actual harm—will proliferate, just as they did after the Partners Healthcare settlement. *See supra* p. 12. And businesses will feel similar pressure to settle meritless claims for significant amounts. In response, businesses may be forced to abandon useful website analytics tools to avoid potential liability, despite their many mutual benefits, harming both businesses and consumers alike.

IV. THE RULE OF LENITY REQUIRES CLARITY BEFORE DEFENDANT'S USE OF PREVALENT TECHNOLOGY IS CRIMINALIZED

The plain language of the Wiretap Act's crime-tort exception clearly requires an intent to commit a *separate* unlawful act beyond the mere act of interception itself. That text alone required dismissal, but to the extent any doubt remains about its meaning, the rule of lenity requires the Court to resolve such doubt in favor of Defendant-Appellee and against civil liability, because the Wiretap Act also carries criminal penalties.

"Under the rule of lenity, grievous ambiguity in a penal statute is resolved in the defendant's favor." *See United States v. Councilman*, 418 F.3d 67, 83 (1st Cir. 2005). The rule thus "vindicates the fundamental principle that no citizen should be held accountable for a violation of a statute whose commands are uncertain." *United States v. Santos*, 553 U.S. 507, 514 (2008) (plurality opinion). And it

preserves "the separation of powers 'by maintaining the legislature as the creator of crimes.'" *Cargill v. Garland*, 57 F.4th 447, 470 (5th Cir. 2023), *aff'd*, 602 U.S. 406 (2024).

Although this is a civil case under the Wiretap Act's private right of action, lenity still applies here because the Act's prohibitions also carry criminal penalties. *See* 18 U.S.C. § 2511(4)(a). Where, as here, a statute "has both criminal and noncriminal applications," the Court must apply the rule of lenity in both situations, so as to "interpret the statute consistently, whether [the Court] encounter[s] its application in a criminal or noncriminal context." *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004); *see also United States v. Thompson/Ctr. Arms Co.*, 504 U.S. 505, 517-518 (1992) (plurality opinion) (applying lenity to "a tax statute that we construe now in a civil setting" because the statute "has criminal applications"); *see also id.* at 523 (Scalia, J., concurring in the judgment) (agreeing that lenity applies in a civil setting). After all, "a statute is not a chameleon" whose meaning can "change from case to case," so "the 'lowest common denominator, as it were, must govern' all of its applications." *Carter v. Welles-Bowen Realty, Inc.*, 736 F.3d 722, 730 (6th Cir. 2013) (Sutton, J., concurring) (quoting *Clark v. Martinez*, 543 U.S. 371, 380 (2005)).

Any theoretical doubt about the meaning of the Wiretap Act's crime-tort exception should thus be resolved in Defendant-Appellee's favor because

Plaintiffs-Appellants' novel, expansive theory of civil liability under the Act would also criminalize the widespread use of industry-standard internet tools and "unintentionally turn ordinary citizens into criminals." *United States v. Nosal*, 676 F.3d 854, 863 (9th Cir. 2012); *see also Staples v. United States*, 511 U.S. 600, 610-616 (1994) (rejecting proposed interpretation of a criminal statute that would criminalize widespread innocent conduct). Plaintiffs-Appellants' interpretation of the Wiretap Act threatens to criminalize the widespread practices of hospitals plus many other healthcare providers and businesses. Applying lenity here would prevent such a destabilizing outcome, ensuring that this Court does not enlarge the scope of the Wiretap Act to reach conduct that Congress did not intend to prohibit in enacting it. *See Williams v. United States*, 458 U.S. 279, 286, 290 (1982) (applying lenity to avoid making "a surprisingly broad range of unremarkable conduct a violation of federal law").

CONCLUSION

The district court's dismissal of the federal Wiretap Act claim should be affirmed.

Respectfully submitted,

/s/ Mark C. Fleming

MARK C. FLEMING
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000
Mark.Fleming@wilmerhale.com

MARIA C. MONAGHAN
MARIEL A. BROOKINS
U.S. CHAMBER LITIGATION CENTER
1615 H Street, NW
Washington, DC 20062
(202) 463-5337

Counsel for Amicus Curiae The Chamber of Commerce of the United States of America

December 18, 2025

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g), the undersigned hereby certifies that this brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B)(i).

1. Exclusive of the exempted portions of the brief, as provided in Fed. R. App. P. 32(f), the brief contains 4,519 words.

2. The brief has been prepared in proportionally spaced typeface using Microsoft Word for Office 365 in 14 point Times New Roman font. As permitted by Fed. R. App. P. 32(g), the undersigned has relied upon the word count feature of this word processing system in preparing this certificate.

/s/ Mark C. Fleming
MARK C. FLEMING
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000
Mark.Fleming@wilmerhale.com

December 18, 2025

CERTIFICATE OF SERVICE

I hereby certify that I filed the foregoing with the Clerk of the United States Court of Appeals for the First Circuit via the Court's CM/ECF system, which will send notice of such filing to all registered CM/ECF users this 18th day of December, 2025.

/s/ Mark C. Fleming
MARK C. FLEMING
WILMER CUTLER PICKERING
HALE AND DORR LLP
60 State Street
Boston, MA 02109
(617) 526-6000
Mark.Fleming@wilmerhale.com

December 18, 2025