COMMONWEALTH OF MASSACHUSETTS
SUPREME JUDICIAL COURT

No. SJC-13542
SUFFOLK COUNTY

KATHLEEN VITA
PLAINTIFF-APPELLEE

v.

NEW ENGLAND BAPTIST HOSPITAL and
BETH ISRAEL DEACONESS MEDICAL CENTER, INC.
DEFENDANTS-APPELLANTS

REPORTED TO THE APPEALS COURT
FROM THE SUPERIOR COURT
DIRECT APPELLATE REVIEW GRANTED

Brief Amici Curiae Of National Consumer Law Center and Electronic Privacy Information Center, In Support Of The Plaintiff-Appellee

---

Attorneys for Amici:

John Roddy, BBO 424240
jroddy@baileyglasser.com
Elizabeth Ryan, BBO 549632
eryan@baileyglasser.com
Bailey & Glasser LLP
176 Federal Street, 5th Floor
Boston, MA 02110
617-439-6730
617-951-3954 (fax)

Table of Contents

Page

Table of Authorities

Page(s)

Cases

Statutes

Regulations

Other Authorities

Corporate Disclosure Statement

Amicus curiae National Consumer Law Center, Inc. is a nonprofit, non-stock corporation. It has no parent corporation, and no publicly traded corporation has an ownership interest in it.

Amicus curiae Electronic Privacy Information Center, Inc., is a nonprofit, non-stock corporation. It has no parent corporation, and no publicly traded corporation has an ownership interest in it.

Statements of Interest of Amici

The National Consumer Law Center ("NCLC") is a national nonprofit research and advocacy organization that works for consumer justice and economic security for low-income and other disadvantaged people, including older adults. NCLC provides information, legal research, and policy analysis to Congress, state legislatures, administrative agencies, and courts. NCLC draws on over fifty years of expertise regarding state and federal deception law and the Fair Credit Reporting Act (FCRA) and its protections for consumers. NCLC publishes Federal Deception Law (4th ed. 2022) and Fair Credit Reporting (10th ed. 2022), which includes information on consumers' privacy rights relating to their medical information.

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention

on emerging privacy and civil liberties issues. EPIC advocates for meaningful regulation of extractive, invasive, and unfair data collection and profiling systems. EPIC regularly files amicus briefs in important privacy cases.

NCLC and EPIC submit this amicus brief to provide the Court with an overview of the core consumer and privacy protections that the Wiretap Act implicates.

Introduction

NCLC and EPIC urge the Court to find that the Wiretap Act, G.L. c. 272, § 99, prohibits the type of surreptitious, undisclosed and unconsented sharing of private health information Appellants ("the Hospitals") are alleged to have engaged in here. Consistent with basic principles of statutory interpretation, buttressed by the public interest in meaningful disclosure, consent and privacy, the tracking software at issue here should be found to be illegal wiretaps. Consumer business that was once conducted in person or over the phone, such as making doctor appointments or inquiring about medical care for specific health concerns, is now conducted online. The privacy interests in these communications has not changed over time. The law needs to keep pace with the rapid technological advances of our digital age, and to make a distinction between telephonic wiretaps and the software trackers at issue here would both hamper enforcement of the Act

and further erode the privacy and consumer protection interests the Act's correct interpretation would provide.

Statement of the Issue

The Wiretap Act prohibits the willful use of an "intercepting device"to secretly intercept the contents of any wire communication. Ms. Vita alleges that the Hospitals used invisible, undisclosed software to track her online interactions with the Hospitals' websites and record and send information to Meta and Google. Does such digital tracking and sharing without consent violate the Wiretap Act?

Summary of Argument

The alleged violations of the Wiretap Act by the Hospitals raise significant consumer privacy and consumer protection issues. Ms. Vita alleges that her online communications with the Hospitals contained private medical information and that the Hospitals both hid the web tracking software and did not disclose that the private medical information she and numerous other consumers provided the Hospitals was shared with advertising giants Meta and Google. The alleged disclosure of this information violates reasonable consumer expectations of privacy, as well as state and federal statutes. Finally, the Hospitals contend that — accepting as true that they surreptitiously track consumers' personal health information and share that information with the tech platforms —nevertheless the consumers subject to these practices are not injured. Accepting this contention

would ignore the realities of how consumers interact with hospital webpages and be a retrenchment to caveat emptor, long repudiated as a distinctly unfair legal principle.

Consumer privacy law prohibits the type of surreptitious, undisclosed and unconsented sharing of private health information alleged here. Consistent with basic principles of statutory interpretation, buttressed by the public interest in meaningful disclosure, consent and privacy, the tracking software at issue here should constitute illegal wiretaps. To make a distinction between telephonic wiretaps and the software widgets at issue here would both hamper enforcement of the Wiretap Act and further erode the privacy and consumer protection interests the Act's correct interpretation would provide.

Argument

I. State and Federal Laws Prohibiting Wiretapping Are Powerful and Important Vehicles to Deter and Remedy Online Invasions of Consumer Privacy

The methods by which people communicate with businesses have changed dramatically over the last several decades. The norm for decades was to use mail and telephone as the primary methods for consumers to conduct their business. But these methods have been substantially superceded by Internet and online communications. Although the methods of communication have changed, consumers' privacy interests in the confidentiality of their communications have

not — especially where sensitive information, such as protected health information is at issue.

The unchanged consumer privacy interest, coupled with the fact that online communications are conducted over wires, has led courts across the county to apply state and federal wiretapping and eavesdropping laws to deter invasions of privacy and to protect consumers' interest in the confidentiality of communications like those at issue here.

For example, the federal Wiretap Act, as amended by the Electronic Communications Privacy Act ("ECPA"), generally prohibits the interception of "wire, oral, or electronic communications." 18 U.S.C. § 2511(1). The Third Circuit Court of Appeals has found the law applied to "a broad scheme in which the defendants generally acquired and tracked the plaintiffs' internet usage," which "involved the collection of at least some 'content' within the meaning of the Wiretap Act." *In re Google Inc. Cookie Placement Consumer Priv. Litig*., 806 F.3d 125, 139 (3d Cir. 2015). This application was confirmed by the Northern District of California in *Brown v. Google LLC*, 525 F. Supp. 3d 1049, 1071 (N.D. Cal. 2021), where plaintiffs alleged that "Google violated the Wiretap Act by intercepting internet communications that Plaintiffs were sending and receiving while they were browsing the internet in private browsing mode." The court held

that plaintiffs "stated a claim for unauthorized interception under the Wiretap Act." *Id.* at 1071.

The Ninth Circuit Court of Appeals has also applied California's wiretap law, the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 631(a), to online communications. *See Javier v. Assurance IQ, LLC*, No. 21-16351, 2022 WL 1744107, at *1 (9th Cir. May 31, 2022). In *Javier*, the plaintiff alleged that he had "visited Nationalfamily.com" and "[t]o request an insurance quote, he answered a series of questions about his demographic information and medical history." *Id.* The Ninth Circuit observed that "[t]hough written in terms of wiretapping, Section 631(a) applies to Internet communications" and, finding plaintiff's allegations that he did not consent to the interception sufficient, reversed the district court's order dismissing the complaint.

The Third Circuit Court of Appeals has also applied Pennsylvania's Wiretapping and Electronic Surveillance Control Act ("WESCA"), 18 Pa. C.S. § 5701, et seq., to online communications. Specifically, in *Popa v. Harriet Carter Gifts, Inc*., 52 F.4th 121, 124 (3d Cir. 2022), the Third Circuit held that the alleged third party interception of information communicated to a retail website was sufficient to allege a violation of the law. *See also Oliver v. Noom, Inc*., No. 2:22-CV-1857, 2023 WL 8600576, at *6 (W.D. Pa. Aug. 22, 2023) (Session Replay Code, "which records website visitors' actions," including information typed by

them while on the Noom website, "falls within WESCA's broad definition of "device.")

The Illinois Eavesdropping Act, 720 Ill. Stat. §§ 5/14-2(a)(3); 5/14-6, has also been applied to internet communications. In *Kurowski v. Rush Sys. for Health*, No. 22 C 5380, 2023 WL 4707184, at *12 (N.D. Ill. July 24, 2023), a case much like the one before the Court, the Northern District of Illinois applied the Illinois Eavesdropping Act, 720 Ill. Stat. §§ 5/14-2(a)(3); 5/14-6, to a healthcare provider where the provider had installed Meta Pixel and similar technology on the provider's website.

These cases from around the country demonstrate that wiretap laws like the Massachusetts Wiretap Act have been and should be applied to protect private online communications such as those alleged by Ms. Vita here. Massachusetts consumers should also benefit from the full scope of protections the Massachusetts Wiretap Act provides for modern communications.

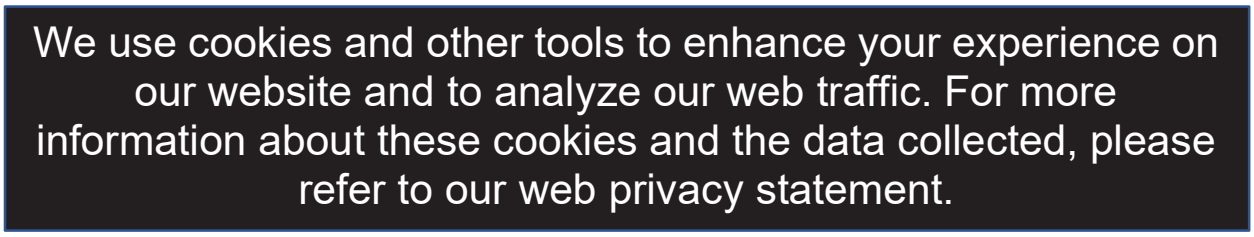
II. Disclosure Plus Consent Would Have Immunized the Hospitals from Wiretap Act Liability, But They Offered Neither

A. If The Hospitals Disclosed that They Invisibly Tracked Consumers and Shared Their Private Health Information, Those Consenting Would Have No Cause to Complain and Those Not Consenting Would Preserve their Medical Privacy

"[T]here is no violation [of Chapter 272] where the recording was not secret, that is, that it was made with the parties' consent or actual knowledge." *Mahoney*

v. DeNuzzio, No. 13-cv-11501, 2014 WL 347624, at *5 (D. Mass. Jan. 29, 2014) (citing *Commonwealth v. Jackson*, 370 Mass. 502, 505-06 (1976)). The Hospitals offer a website pop-up and an opaque privacy notice in their defense. The Hospitals' Opening Brief, at 16, provides:

> Plaintiff alleges that the presence of AdTech was "secret," but it is undisputed that each website displayed the following pop-up notice:



> That notice linked to a longer privacy policy, which included content such as:
>
> ***[BIDMC/NEBH] routinely gathers data on website activity … We and our Third Party Service Provider collect and save the default information customarily logged by worldwide web server software***. Our logs contain the following information for each request: date and time, originating IP address and domain name (the unique address assigned to your Internet service provider's computer that connects to the Internet), object requested …

The Hospitals contend they "***did*** disclose the collection of browsing data by themselves and at least one third party." *Id*., at 33. But nowhere does the privacy policy use the term "browsing data." And even if it did, neither the term "browsing data" nor the terms actually used in the policy clearly convey to a consumer that their searches for medical specialists, symptoms and treatments would be collected and disclosed to third parties. To a consumer, the terms used in the policy refer to

mundane technical data, not their sensitive private health information. Nor does "our Third Party Service Provider" clearly and conspicuously disclose that the private health information the Hospitals collect would be shared with Meta and Google.

A consumer must be given the opportunity to consent, and where the choices are not made clear and conspicuous, consent may not be obtained. In *Cullinane v. Uber Techs., Inc*., 893 F.3d 53, 63 (1st Cir. 2018), the First Circuit posed the following questions in the process of finding that Uber's opaque and difficult-to-access arbitration provision was neither clearly disclosed nor consented to by a proposed class of consumers:

> In examining the interface, we evaluate the clarity and simplicity of the communication of the terms. Does the interface require the user to open the terms or make them readily available? How many steps must be taken to access the terms and conditions, and how clear and extensive is the process to access the terms? *Id*., at 62 (citations omitted).

Ms. Vita alleges that the Hospitals deploy the Meta Pixel and Google Analytics to collect patient information to target advertising to that individual, and that the Hospitals derive significant benefit from those software tracking tools, including better targeted advertising. The Hospitals' tepid boilerplate alluding to "browsing data" and "unidentified third party service provider[s]" comes nowhere close to telling consumers what is really being done with their private medical information.

The Hospitals respond that consent was implicit in the context, and that just by using the website (coupled with the "disclosures" described above) Ms. Vita effectively consented to the tracking and sharing. Opening Brief, at 43. There are two reasons this contention is misguided. First, the context here includes the Hospitals' Privacy Policy[1] assurances that consumers' personal health information is well-protected and confidential.

> We have taken reasonable steps to ensure the integrity and confidentiality of personally identifiable information you voluntarily and explicitly provide ….
>
> Beth Israel Deaconess Medical Center routinely gathers data on website activity, such as how many people visit the site, the pages they visit, where they come from, how long they stay, etc. The data is collected on an aggregate, *anonymous basis, which means no personally identifiable information* is associated with the data. This data helps us improve site content and overall usage. This *information is not shared with other organizations*. (emphases added).

One way to view the Privacy Policy in the context of Ms. Vita's case is that its assurances contradict, or at least are inconsistent with, the software tracking and sharing practices she alleges the Hospitals engage in. A federal consumer protection law, the Fair Debt Collection Practices Act, 15 U.S.C. § 1692g, expressly prohibits disclosures that "overshadow" a consumers' rights. See, e.g., *Pollard v. L. Off. of Mandy L. Spaulding*, 766 F.3d 98, 105 (1st Cir. 2014) (deceptive debt collection letter effectively overshadowed the statutorily required

[1] https://www.bidmc.org/privacy-policy

disclosure of consumer's right to dispute debt). This is but another way of describing the core consumer law principle of requiring clear and conspicuous disclosure of consumer rights.

Second, the notion that visiting the website equates to consent invokes a so-called "browsewrap" agreement, where just visiting a website constitutes consent to terms contained therein. In another Uber arbitration case this Court noted that such implicit consent agreements have "been held to be unenforceable" because "there is no assurance that the user was ever put on notice of the existence of the terms or the link to those terms." *Kauders v. Uber Techs., Inc*., 486 Mass. 557, 579 n. 26 (2021). "Ultimately, the offeror must reasonably notify the user that there are terms to which the user will be bound and give the user the opportunity to review those terms. *Id*., at 573.

Procuring consumers' consent "is not hard to accomplish, as the enormous volume of commerce on the Internet attests." *Sgorous v. TransUnion Corp*., 817 F.3d 1029, 1036 (7th Cir. 2016); *see also Javier v. Assurance IQ, LLC*, 649 F. Supp. 3d 891, 900 (N.D. Cal. 2023) (obtaining consent "when visiting websites (for the collection of cookies, for example) is a regular occurrence and hardly particularly 'technologically impractical.'").

B. The Hospitals Foretell Economic Calamity Should They Be Held to Account But Can Avoid This Imagined Catastrophe By Obtaining "Prior Authority"

The Hospitals see "calamitous consequences across all for-profit and non-profit sectors of the Massachusetts economy" arising should the Court side with Ms. Vita. Opening Brief, at 28. But those imagined devastating effects are avoided by simply disclosing the tracking software, the information they capture and share with Meta and others and obtaining consent. *See* G.L. c. 272, § 99(b)(4) (allowing interception if given "prior authority").

Nevertheless, the Hospitals contend that Ms. Vita's "'just disclose' solution does not address the massive *retrospective* liability her legal theory would create." Opening Brief, at 34 (emphasis in original). In other words, even though the Hospitals could fix their websites going forward to procure consent for future wiretapping, they complain that holding them accountable for existent violations is somehow unfair. Worse, the Hospitals ignore the fundamental risk they have created for their patients: once the Hospitals share their patients' medical information with Meta and Google they have no way to monitor or control what happens to it afterward. As The Wall Street Journal recently observed, "[m]any corporations have relationships with data brokers and sell or trade information

about [] customers."[2] There is nothing to stop companies like Meta from selling patients' health data to insurance companies or employers who wish to screen individuals for potential health risks. Nor is there anything preventing Meta and Google selling such information in bulk to companies who wish to exploit it for other purposes.

The alleged privacy violations here resulted from conscious choices by the Hospitals to ignore HIPAA's express prohibition against unauthorized disclosure of patients' health information for "Marketing" purposes. *See* 45 C.F.R. § 164.508. By encouraging patients to use their websites, then sharing their patients' health data with Meta and Google for advertising benefits, the Hospitals forfeited any claim to unfair treatment here. After having made their bargain with the tech giants, the Hospitals are hardly in a position to argue that their *patients* should be denied a remedy.

As the Hospitals concede, the Massachusetts Wiretap Act has been the law for nearly 70 years. Opening Brief, at 31. They certainly can (and should) fix their practices going forward, but there is no excuse for their failure (or refusal) to do so in the past, and the Hospitals should bear responsibility for their cavalier collection and distribution of private medical information to Meta and Google.

---

[2] Byron Tau, "U.S. Spy Agencies Know Your Secrets. They Bought Them," WALL ST. JOURNAL, March 9, 2024, at C1.

III. The Non-Consensual Sharing of Private Medical Information With Meta and Google Invades Consumers' Privacy, An Injury That Provides Standing

The Hospitals frame the standing issue as whether a standalone, plausibly alleged Wiretap Act violation, without more, is sufficient to confer standing. But this frame doesn't capture the crux of this case —the Hospitals' alleged surreptitious recording of their *patients'* communications involving symptoms and inquiries about medical issues. These alleged disclosures to third parties for reasons unrelated to medical treatment are a violation of consumers' substantive rights to privacy.

Private health information is among the most sensitive information a consumer may disclose. For that reason both state and federal law require health providers to protect the confidentiality of a patient's private health records and communications. Those same laws strictly limit the provider's disclosure of such information to third parties without consent. *See* G.L. c. 111, § 70E (patients' and residents' rights); Health Information Portability and Accountability Act ("HIPAA"), Pub. L. No. 104-191 (1996). So, here, the issue is whether patients like Ms. Vita reasonably expect that when seeking information from the website about specific symptoms, conditions, and medical procedures (Opening Brief, at 16) that their inquiries about such medical issues would be automatically shared with Meta and Google.

No reasonable person would expect such sharing, which is precisely why the law requires consent before any such information may legally be shared. "When individuals are not informed of their rights or not given important information, they are harmed because they lose their ability to assert their rights at the appropriate times, to respond effectively to issues involving their personal data, or to make meaningful decisions regarding the use of their data." Danielle Citron, Daniel Solove, *Privacy Harms*, 102 Boston University Law Review 793, 849 (2022). Ms. Vita alleges that the Hospitals did not obtain her consent, and that she had no idea that her inquiries about symptoms, conditions and procedures were being tracked via the software at issue here.

The harm caused by the secret recording and sharing of Ms. Vita's personal health information, also has a close relationship to the harm that the tort of intrusion upon seclusion protects against. *See* Restatement of the Law, Second, Torts, § 652B. In fact, a wiretap is a classic example of an intrusion upon seclusion. *Id*. (listing the "tapping of telephone wires" as an example of an intrusion upon seclusion.)[3] So, even under the more stringent requirements of Article III, Ms. Vita has standing to pursue her claims in this case. *See TransUnion v. Ramirez*, 594 U.S. 413, 425 (2021)(recognizing that an injury with a close

[3] *See* Citron and Solove's "typology of privacy harms" for an enumeration of the various forms of harm that privacy intrusions inflict. *Id*., at 831.

relationship to intrusion upon seclusion meets Article III's standards for concreteness). Similarly, pleading disclosure of private information can also provide plaintiffs with standing in Article III courts. *Id*. (listing "disclosure of private information" as a harm traditionally recognized as providing a basis for a lawsuit in American courts.)

Ms. Vita and other consumers who allege the Hospitals didn't disclose the tracking and didn't obtain their consent, thereby violating their privacy rights, have suffered the requisite injury to establish standing. "To have standing in any capacity, a litigant must show that the challenged action has caused the litigant injury" [citation omitted]. *See Sullivan v. Chief Justice for Admin. & Mgt. of the Trial Court*, 448 Mass. 15, 21 (2006). And that injury must be more than merely "speculative, remote, and indirect." *Id*.

Federal regulators have repeatedly warned healthcare providers about installing and using these sorts of tracking technologies on their public-facing websites and stated that doing so may be a violation of patients' and website users' privacy. On March 16, 2023, the Federal Trade Commission ("FTC") Office of Technology issued a blog post titled "Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking," in which the FTC provided cautionary warnings about the use of tracking pixels, such as the Meta Pixel, and the serious privacy

violations such tracking causes.[4] On July 20, 2023, the FTC and the U.S. Department of Health and Human Services' Office for Civil Rights ("OCR"), took further action, sending a "joint letter to approximately 130 hospital systems and telehealth providers to alert them about the risks and concerns about the use of technologies, such as the Meta/Facebook pixel and Google Analytics, that can track a user's online activities. These tracking technologies gather identifiable information about users, usually without their knowledge and in ways that are hard for users to avoid, as users interact with a website or mobile app."[5]

"As more people learn how much of their personal information is in the hands of strangers with algorithms, they become concerned."[6] For instance, when Apple gave iPhone users a clear, conspicuous, and simple way to opt out of mobile

---

[4] *See Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, FEDERAL TRADE COMMISSION (Mar. 16, 2023), https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking.

[5] *See FTC and HHS Warn Hospital Systems and Telehealth Providers about Privacy and Security Risks from Online Tracking Technologies*, FEDERAL TRADE COMMISSION (JULY 20, 2023), https://www.ftc.gov/news-events/news/press-releases/2023/07/ftc-hhs-warn-hospital-systems-telehealth-providers-about-privacy-security-risks-online-tracking.

[6] Marcus Moretti and Michael Naughton, *Why Privacy Policies Are So Inscrutable*, THE ATLANTIC (Sept. 5, 2014), https://www.theatlantic.com/technology/archive/2014/09/why-privacy-policies-are-so-inscrutable/379615/.

applications tracking them for targeted advertising, "62% [] opt[ed]-out."[7] Similarly, "79% of adults assert they are very or somewhat concerned about how companies are using the data they collect about them."[8] And "[b]oth the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person." *United States Dep't of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 763 (1989).

And this level of consumer concern involves the ubiquitous run of the mill tracking that leads to seeing ads about wingtips appear shortly after a search for "nice, dress shoes." So, a consumer who seeks information about, e.g., ovarian cancer, or who searches for a doctor experienced in treating HIV, is injured when that highly sensitive private information is shared with Meta and Google.

That injury is tangible, visceral and direct. As the Hospitals acknowledge, "the Privacy Act[9] … was enacted for the explicit purpose of protecting individuals 'against ***unreasonable, substantial or serious*** interference[s] with [their]

---

[7] Kif Leswing, Apple's Ad Privacy Change Impact Shows The Power It Wields Over Other Industries, CNBC (Nov. 13, 2021), https://www.cnbc.com/2021/11/13/apples-privacy-changes-show-the-power-it-holds-over-other-industries.html

[8] Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RESEARCH CENTER (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[9] G.L. c. 214, § 1B.

privacy.'" Opening Brief, at 32 (emphasis in original). And where, as here, a plaintiff alleges a systematic, unreasonable, substantial and serious sharing of thousands of similar consumers' private health information, a court "may determine, particularly when class actions are involved, that concerns other than standing, in its most technical sense, may take precedence." *See Weld v. Glaxo Wellcome Inc.*, 434 Mass. 81, 88 (2001).

Conclusion

NCLC and EPIC support Ms. Vita's interpretation of the Wiretap Act because it protects important consumer privacy interests in the confidentiality of sensitive communications, is consistent with interpretations of similar wiretap statutes across the country, and because the Hospitals engaged in deceptive conduct that was injurious to their patients. The Court should hold that Ms. Vita and similar consumers have standing and that the Wiretap Act applies to these communications.

Dated: March 13, 2024

Respectfully submitted,

National Consumer Law Center and Electronic Privacy Information Center,

By their attorneys,

/s/ John Roddy
John Roddy, BBO 424240[10]
jroddy@baileyglasser.com
Elizabeth Ryan, BBO 549632
eryan@baileyglasser.com
Bailey & Glasser LLP
176 Federal Street, 5th Floor
Boston, MA 02110
617-439-6730
617-951-3954 (fax)

Certificate Of Compliance

Pursuant to Rule 17(9) of the Massachusetts Rules of Appellate Procedure, I hereby certify that this brief complies with Rules 17 and 20 of the Massachusetts Rules of Appellate Procedure. This brief has been produced in 14-point Times New Roman font and contains 4,010 non-excluded words. The brief was created using Microsoft® Word for Mac, Version 16.82.

Dated: March 13, 2024

/s/ John Roddy
John Roddy

Certificate Of Service

Pursuant to Rule 13(e) of the Massachusetts Rules of Appellate Procedure, I hereby certify that on March 13, 2024, this document was served upon all counsel of record via the Massachusetts Tyler Host electronic filing system.

Dated: March 13, 2024

/s/ John Roddy
John Roddy

[10] The undersigned counsel neither represents nor has represented any of the parties to the present appeal in another proceeding involving similar issues, nor was a party or represented a party in a proceeding or legal transaction that is at issue in the present appeal within the meaning of Mass. R. App. P. 17(c)(5)(C). Nevertheless, in the interest of full disclosure the undersigned informs the Court that he is plaintiff's counsel in a putative Wiretap Act class action against the Steward hospital system, *Jane Doe v. Steward Health Care System LLC*, Suffolk Superior Court, Civil No. 2384CV00174-BLS1, a case not identified in footnote 9 of the trial court's Memorandum of Decision.