# Supreme Judicial Court

FOR COMMONWEALTH OF MASSACHUSETTS
No. SJC-13542

Suffolk, ss.

---

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 FOR AMICI CURIAE
THE GREATER BOSTON CHAMBER OF COMMERCE AND
MASSACHUSETTS NONPROFIT NETWORK
SUPPORTING APPELLANTS**

---

Elka T. Sachs (BBO# 562007)
Krokidas & Bluestein LLP
600 Atlantic Avenue, 19th Floor
Boston, MA 02210
617-482-7211
ets@kb-law.com

Attorney for the Massachusetts Nonprofit Network

Ian D. Roffman (BBO# 637564)
Seth P. Berman (BBO# 629332)
Natalie M. Cappellazzo (BBO# 699355)
Natalia Peña (BBO# 707596)
Nutter McClennen & Fish LLP
155 Seaport Boulevard
Boston, MA 02210
617-439-2000
iroffman@nutter.com
sberman@nutter.com
ncappellazzo@nutter.com
npena@nutter.com

Attorneys for the Greater Boston Chamber of Commerce

Date: March 13, 2024

## CORPORATE DISCLOSURE STATEMENT

*Amicus Curiae*, the Greater Boston Chamber of Commerce, is an independent, non-profit business association representing more than 1,300 businesses throughout the region. It has no parent corporation and no publicly held corporation owns 10% or more of its stock.

*Amicus Curiae*, the Massachusetts Nonprofit Network, is an independent, non-profit association representing more than 600 Massachusetts member organizations, 500 of which are nonprofits and 100 provide services to nonprofits. It has no parent corporation and no publicly held corporation owns 10% or more of its stock.

## TABLE OF CONTENTS

## TABLE OF AUTHORITIES

**Page(s)**

**Cases**

**Statutes**



**Other Authorities**

## IDENTITY AND INTEREST OF AMICI CURIAE THE GREATER BOSTON CHAMBER OF COMMERCE AND THE MASSACHUSETTS NONPROFIT NETWORK

The Greater Boston Chamber of Commerce ("GBCC" or "Chamber") is an independent, non-profit organization that is the convener, voice, and advocate of the Greater Boston business community. The Chamber represents more than 1,300 businesses of all sizes from virtually every industry and profession in the Greater Boston region.

The Chamber is committed to driving the region's economic growth and prosperity by ensuring that Massachusetts remains a competitive place to start, expand, and run a business. One key element of the Commonwealth's competitiveness is maintaining consistency with federal law and other states on legal issues that can affect businesses. If Massachusetts adopts a policy that is an outlier in exposing businesses in the Commonwealth to litigation risks and costs higher than those found in other states, Massachusetts risks losing out on future growth.

The Massachusetts Nonprofit Network ("MNN") is a nonprofit statewide association that acts as the voice of the nonprofit sector by synthesizing all parts of the nonprofit ecosystem -- organizations, funders, community and business leaders, and elected officials -- to protect and strengthen nonprofits, and raise the sector's voice on critical issues. MNN has more than 600 members, representing nonprofits

in every region of the Commonwealth, and in all sub sectors including healthcare, human services, housing, education, and civic engagement.

The nonprofit sector employs roughly 18% of the Commonwealth's workforce and provides essential services and benefits to our communities and populations in-need. Through the pandemic and after years of tireless direct services work, many nonprofits are experiencing a strain on their ability to attract and retain their workforce. Additionally, with rising costs and more administrative pressures than ever, nonprofits budgets are waning. This litigation potentially exposes nonprofits to an additional unexpected threat to their sustainability.

*Amici* are advocates for thoughtful legislation to protect consumer data and privacy nationwide, but they have significant concerns about policy approaches that authorize private rights of action, criminalize ordinary business practices, and create a different standard for entities in the Commonwealth than in other states.

*Amici* believe that the trial court's decision creates significant and unreasonable potential civil and criminal liability for thousands of Massachusetts for-profit and nonprofit businesses and have significant concerns about the potential impact that the trial court's decision could have on the nonprofit sector and its ability to provide essential support and services to those in need. *Amici* therefore submit this *Amici Curiae* brief urging that the decision below be reversed.

## RULE 17(C)(5) DECLARATION OF AMICI AND COUNSEL

*Amici Curiae* and their counsel declare that:

A. No party or party's counsel authored this brief in whole or in part;

B. No party or party's counsel contributed money that was intended to fund the preparation or submission of this brief;

C. No person or entity -- other than the *Amici Curiae*, their members, or their counsel -- contributed money that was intended to fund preparing or submitting this brief; and

D. Neither the *Amici Curiae* nor their counsel represents or has represented one of the parties to the present appeal in another proceeding involving similar issues or was a party or represented a party in a proceeding or legal transaction that is at issue in the present appeal.

## POSITION OF AMICI CURIAE

The Chamber and MNN urge reversal of the Superior Court's decision. *Amici* and their members share the concern of all Massachusetts citizens and taxpayers over protecting consumer data and privacy. But a jerry-rigged interpretation of the 1968 Wiretap Act, which could not possibly have been intended to regulate the use of advertising technology on the internet, is not the way to do it.

*Amici* believe that the Superior Court's decision is contrary to this Court's recent cases that narrowly interpret the Wiretap Act, and that the decision is contrary to the legislative intent of the Wiretap Act, which was intended to criminalize surreptitious eavesdropping on the content of two-party conversations. The decision ignores that website browsing is fundamentally different from telephone calls and other conversations contemplated when the Wiretap Act was enacted in 1968: it is a multi-party activity involving publicly-accessible servers that commonly involves notice to the user about the use of "cookies" and other technologies that monitor online activity. If the Superior Court's decision were to stand, Massachusetts businesses would be at a severe competitive disadvantage to businesses located in other states because nearly ubiquitous internet advertising activity would subject businesses in the Commonwealth to massive penalties while their out-of-state competitors who engage in exactly the same conduct would be exempt. Indeed, the out-of-state businesses would be expressly exempted *even if they targeted*

*Massachusetts consumers* because the Wiretap Act by its terms does not cover monitoring activities that occur partially out of state.

For these reasons, *Amici* urge this Court to reverse the Superior Court's decision.

## ARGUMENT

Plaintiffs seek to use the 1968 Wiretap Act to retroactively regulate a now nearly ubiquitous internet tracking technology. Their anachronistic reading of the Wiretap Act stands in sharp contrast to the Legislature's stated intent in passing the Act, ignores the reality of how the internet works, and violates the due process rights of organizations throughout the Commonwealth. Reading the Act that way would lead to perverse results: a rush to the courthouse to force Massachusetts-based companies to pay enormous statutory damages even in the absence of a showing of any actual harm, while companies based outside Massachusetts who have engaged in exactly the same conduct *intentionally directed toward Massachusetts consumers* would be entirely free from liability because the statutory text does not apply to interceptions occurring outside the Commonwealth. Making matters worse, the statute's three-year statute of limitations ensures that there is nothing Massachusetts organizations can now do to prevent being sued for their past use of this commonplace technology. Simply put, the Plaintiffs' interpretation of the statute will open the floodgates of litigation against organizations throughout the

Commonwealth, amounting to a grossly unfair tax on Commonwealth organizations and a concomitant windfall for plaintiffs and their lawyers. And because the Wiretap Act is a criminal statute, Plaintiffs' interpretation would mean that hundreds of businesses and thousands of individuals would be subject to arrest and prosecution for a common and ordinary business practice.

## I. The Wiretap Act Must be Read in Light of its Legislative History to Discern the Legislature's Intent

Plaintiffs' reading of the Wiretap Act contradicts the statute's legislative history and intent, and it ignores this Court's admonition that the Wiretap Act must be interpreted in light of its legislative history, not merely through an analysis of its text. *Curtatone v. Barstool Sports, Inc.*, 487 Mass. 655, 659 (2021).

### A. The Legislature Significantly Revised the Wiretap Act In 1968 to Prevent Eavesdropping on Private Conversations

The first iteration of the Massachusetts wiretap statute appeared in 1920. *See Com. v. Tavares*, 459 Mass. 289, 294 (2011). The statute was substantially revised in 1959 and overhauled again in 1968. *Com. v. Ennis*, 439 Mass. 64, 69 n.9 (2003). The 1968 amendments to the statute were introduced following a study conducted by the Special Commission on Electronic Eavesdropping. *See id*. The Legislature's objectives, declared in the statute's preamble, were twofold: "to (1) curtail 'the uncontrolled development and unrestricted use of modern electronic surveillance devices,' which the Legislature termed a danger 'to the privacy of all citizens,' and

to (2) combat the 'grave danger to the public welfare and safety' and 'legitimate business activities' posed by 'the increasing activities of organized crime.'" *Tavares*, 459 Mass. at 295 (quoting *Com. v. Thorpe*, 384 Mass. 271, 276–277 (1981)). The Special Commission's report suggested at least two reasons for the second enumerated concern: (1) "the commission heard testimony that newly developed inventions, 'eavesdropping devices' and 'bugs,' could be easily concealed and used to monitor private conversations secretly and continuously," which prompted concern that even a person with "minimal education in electronics" could easily install such widely-available devices to illegally intercept communications, and (2) the Special Commission learned that the New England Telephone and Telegraph Company had been secretly recording private telephone calls to monitor customer service. *Ennis*, 439 Mass. at 69 n.10.

### B. The Legislature's Intent to Protect the Privacy of Conversations Cannot be Squared with the Superior Court's "Overly Literal" Reading of the Wiretap Act

That legislative history is important because it has informed how this Court -- and others across the Commonwealth -- have interpreted and applied the Wiretap Act in the decades since its current form took shape in 1968. Where there is any ambiguity in the plain meaning of the language of a statute, courts will endeavor to read it "in harmony with common sense and sound reason and consistent with legislative intent." *Curtatone*, 487 Mass. at 659 (quoting *Commonwealth v. Gomes*,

483 Mass. 123, 127 (2019)). This principle is especially applicable to the Wiretap Act because the legislative intent behind the statute is "apparent both in the legislative history of the act ***and*** the act itself." *Id*. (emphasis added). In other words, interpretation of the Act must be consistent not only with a common sense reading of the text of the statute but also with its legislative intent and history. Although the statute's definitions may be broad, the legislative history of the Wiretap Act -- and cases analyzing it -- confirms that a narrower reading of the law was intended as it relates to proscribed conduct. As another judge of the Superior Court noted in January of this year, "Despite its broad terms, our courts do not apply an overly literal construction of that statute, which would prohibit large swaths of activity the Legislature did not intend to forbid." *Com. v. Daphnis*, No. 2184CR00160, 2024 WL 486275, at *8 (Mass. Super. Ct. Jan. 8, 2024) (finding the Wiretap Act inapplicable to Snapchat posts).

This Court rejected a literal interpretation of the Wiretap Act in *Commonwealth v. Gordon*. *See* 422 Mass. 816, 832–33 (1996). In *Gordon*, this Court held that although the statute could be read literally to prohibit the secret audiotaping of booking procedures, the Court was unwilling to find such intent by the Legislature in the absence of more specific language in the statute:

> Although G.L. c. 272, §§ 99 B 4 and 99 C 1, can be read literally as making unlawful the audiotaping of booking procedures without the knowledge of the persons being booked, and as subjecting the responsible police officers to severe penalties therefor, in the absence of more specific statutory language

> to that effect and in light of the preamble, ***we are unwilling to attribute that intention to the Legislature***. It is apparent from the preamble that the legislative focus was on the protection of privacy rights and the deterrence of interference therewith by law enforcement officers' surreptitious eavesdropping as an investigative tool. It is in that context that the Legislature limited police use of electronic surveillance (investigative) devices to the investigation of organized crime "under strict judicial supervision." The Legislature does not appear to have had in mind the recording of purely administrative bookings steps following an individual's arrest.

*Gordon*, 422 Mass. at 832–33 (emphasis added). Holding that the Legislature intended to bring AdTech -- the internet advertising technology at issue here -- within the ambit of the statute requires an even further leap than extending the Wiretap Act to criminal booking procedures. If this Court could not discern such an intent in *Gordon*, it is impossible to imagine that the Legislature would have intended to capture AdTech when it amended the law in 1968, whether or not a "literal" reading of the statute in 2024 could arguably support such a prohibition.

### C. *Rainey* and *Morris* also Looked to Legislative Intent to Reject an Overly Literal Construction of the Wiretap Act

This Court has continued to recognize that the Wiretap Act ought to be understood to cover only those actions that violate the core protection provided by the statute. Two cases from last year illustrate this point. In *Rainey*, the Court held that an officer's use of a body-worn camera to record a domestic assault victim's report of the assault and later use of that footage at the defendant's probation violation proceeding did not violate the Wiretap Act. *See Commonwealth v. Rainey*, 491 Mass. 632, 647 (2023). In *Morris*, the Court similarly found that the recording

of a defendant's interview at the police station did not violate the statute. *See Commonwealth v. Morris*, 492 Mass. 498, 506 (2023).

The Superior Court below distinguished the *Rainey* and *Morris* decisions on the grounds that unlike in those cases, the website users here "are not alleged to be proceeding with the implicit understanding that their communications are to be preserved and memorialized, electronically or by handwritten notes, by a government body, for important public safety reasons." October 31, 2023 Memorandum of Decision and Order on Defendant's Motion to Dismiss and Report to the Appeals Court ("Order") at 9.

The Superior Court's Order instead relies on what it sees as the "broad language" of the statute's preamble and reads this Court's decision in *Moody* as having endorsed a "broad interpretation of the statute's language." (Order at 9–10.)[1] But an important distinction lies in the language from *Moody* on which Superior Court relies: although *Moody* acknowledged that the statutory *definitions* in the Wiretap Act are broad, it did not go so far as to say that the statute as a whole should be read broadly, particularly when doing so would sweep in conduct that the Legislature could never have contemplated. *See generally Com. v. Moody*, 466

[1] The Superior Court stated, "[i]n light of the broad statutory definitions of the terms 'wire communication' and 'interception,' we conclude that the Massachusetts wiretap statute provides protection for the electronic transmission of text messages." *Id*. (quoting *Com. v. Moody*, 466 Mass. 196, 209 (2013)).

Mass. 196. Rather, *Moody* simply held that the statutory definitions of "wire communication" and "interception" were broad enough to encompass cell phone calls and text messages. *See id*. at 207, 209. As to cell phone calls, the Court found: "We have no doubt that, in enacting the Massachusetts wiretap statute, the Legislature intended to protect all calls that to any extent or degree traveled 'by the aid of wire, cable, or other like connection.' The reality that cellular telephone technology has drastically reduced the need for such connections does not alter the 'intrinsic intended scope' that we read the statute to preserve." *Id*. at 207. And as to text messages, the Court held: "Infused by the ordinary meaning of the term 'record,' it is apparent that the Legislature's use of the phrase 'secretly record' includes the interception of text messages by viewing and transcribing them for use at a later date." *Id*. at 209.

It is worth revisiting *Rainey* and *Morris* against the backdrop of the Legislature's intent. Both cases echo the familiar sentiment that courts will not deploy an overly literal reading of the Wiretap Act that strays from the Legislature's intent. This Court in *Rainey* acknowledged that a literal reading of the law could support the defendant's position on body-camera footage ("Admittedly, subsection 99 C of the wiretap statute could be construed literally as the defendant suggests, subjecting police officers, probation officers, prosecutors, and the judge to severe penalties" (*Rainey*, 491 Mass. at 642)), but that nothing in the statute -- including

the preamble -- reflected that the Legislature intended to prohibit that conduct. *Id*. at 642–643. The Court found that the same was true of the statute's legislative history:

> The Legislature's focus was the use of devices, like bugs, for clandestine or surreptitious eavesdropping; the Legislature ***did not appear to have in mind*** law enforcement officers' use of devices to record a crime victim's voluntary reporting of a crime under circumstances where, as here, the victim understood her statement was being preserved by them. In sum, the legislative history (like the statutory framework, including the preamble) is ***devoid of anything to support the defendant's proposed construction***, and accordingly, we reject it.

*Id*. at 646–647 (emphasis added).

Several months later, this Court applied a similar analysis in *Morris*. There, this Court explained that it had acknowledged in *Rainey* that a literal reading of the statute could criminalize the conduct at issue, but that it declined to adopt such a construction "given the absurdity of such a result." *Morris*, 492 Mass. at 505. The Court reiterated its conclusion that the Legislature "did not have in mind" the type of voluntary statement that was given by the victim in *Rainey*, and reached the same conclusion about the recording of the defendant's interrogation in *Morris*: "Similarly, here nothing in the statute as a whole, including its codified preamble, supports the conclusion that the Legislature intended to criminalize the police officers' recording of the defendant's voluntary statement, which the defendant understood was being preserved for future use in connection with the investigation of the crime about which the defendant was speaking voluntarily." *Id*. at 506.

The Superior Court putatively distinguished *Morris* and *Rainey* on the factual grounds that the Plaintiffs here are not alleged to have understood that their communications were being preserved and memorialized by the government for public safety reasons. (Order at 9.) But that ignores the tenet of statutory interpretation underpinning both decisions. *Morris* and *Rainey* pose this fundamental question: Even if a literal reading of the statute could plausibly support a prohibition of certain conduct, can it be said that the Legislature "had in mind" that conduct? Here, as in *Gordon*, *Morris*, and *Rainey,* the answer is "no." *Morris*, 492 Mass. at 506 n.9 ("Our reasoning in *Gordon*, as we explained in *Rainey*, centered on the Legislature's intent, as evinced in the wiretap statute's preamble … to prohibit surreptitious eavesdropping; because the Legislature did not appear to have in mind the recording of a booking procedure at the police station, we did not adopt the literal construction urged by the defendant") (internal citations omitted). If the Legislature did not intend for the Wiretap Act -- a primarily criminal statute -- to capture recordings of criminal bookings (*Gordon*), body camera footage (*Rainey*), or recordings of interrogations (*Morris*), it is impossible to believe that it intended the statute to act as a means of regulating ubiquitous internet commerce technology.

## II. Websites Visits are Multiparty Interactions, Not Two-Party Conversations

Plaintiffs ignore the fundamental reality of how the internet and AdTech work in trying to shoehorn this technology into a 1968 statute focused on audio recordings and telegrams. Unlike telephone and telegram conversations, website visits are not two-party "conversations." A website is typically made up of content from several sources, and accordingly, interacting with that website means interacting with several different parties. For example, the Boston Globe website contains its own curated content, but also content from advertisers, links to other websites with source material, and videos hosted by yet additional providers. Websites like Google News and Apple News collect articles from various publications and post them on one website. Kayak displays offers from multiple travel booking platforms. Thus, visiting a website is not a private one-on-one interaction between the user and the company that owns the website. Plaintiffs' claims ignore this reality, and instead pretend that this multiparty interaction is actually a two-party conversation.

### A. The Information Tracked in the Course of Web Browsing Does Not Record the Substance of Any Communication

Plaintiffs' argument also relies on pretending that the act of website browsing is really a form of conversation. This does not comport with either the users' perception of the experience or the categories of communication described in the Wiretap Act. The statute defines interception as "secretly hear[ing], secretly

record[ing], or aid[ing] another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device by any person other than a person given prior authority by all parties to such communication." G.L. c. 272, § 99(B)(4). The data recorded from tracking of a user's movements on a website are not "contents" as defined in the statute. "Contents" is defined as "any information concerning the identity of the parties to such communication or the existence, contents, substance, purport, or meaning of that communication." G.L. c. 272, § 99(B)(5). Although a website itself may communicate certain information, the act of accessing a website to read what might be posted there is not "content" in substance or meaning nor is it a "communication" in any normal sense of the word.

Plaintiffs allege that information being logged includes IP addresses, "information about which pages are visited, which links/buttons are clicked, which menu selections are made, and sometimes which words are typed into search boxes or form fields and/or how far down a webpage a visitor scrolls." (Def. Br. at 13.) These data about web browsing do not constitute communications like the telephone or telegram interception prohibited by the Wiretap Act. Rather, the information conveyed is more analogous to surveillance footage at a retail store that shows customers' time in a store, the aisles they were in, and the items they purchased. Indeed, courts in other jurisdictions that have considered similar issues have not understood browsing activity to be the content of communications. *See*, *e.g.*,

*Goldstein v. Costco Wholesale Corp*., 559 F. Supp. 3d 1318, 1321 (S.D. Fla., 2021) ("mere tracking of Plaintiff's movements on Defendant's website is the cyber analog to record information Defendant could have obtained through a security camera at a brick-and-mortar store."). Further, courts have routinely held that URL tracking is not substantive information subject to wiretap statutes. *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 275 (3d Cir. 2016) (affirming dismissal of wiretap claim and distinguishing URLs that "may convey substantive information" from those that convey "mere dialing, routing, addressing, or signaling information") (quotations omitted); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (comparing numbers dialed on a telephone in pen register cases to "instructions ... voluntarily turned over" to a computer server for the "purpose of directing the routing of information"); *see also In re Facebook Internet Tracking Litigation*, 140 F. Supp. 3d 922, 935–36 (N.D. Cal. 2015) (finding that the tracking of the websites users visited did not constitute "content" under the Electronic Communications Privacy Act).

Similarly, courts have held that even very sensitive data automatically generated in connection with phone calls do not meet the definition of "content" in wiretap statutes. In *In re iPhone Application Litig.*, the plaintiffs alleged that Apple violated the ECPA by collecting information about the precise geo-location data of iDevice users through cell phone towers, Wi-Fi transmissions, and the GPS data on

the plaintiffs' devices. 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012). The court disagreed that this type of data constituted content, ruling that "the identities of parties to a communication and other call data" were not "content." *Id*. The court analogized the data Apple collected with data automatically collected during phone calls -- such as the call's start time and duration -- which it held did not constitute content. *Id*. (citing *United States v. Reed,* 575 F.3d 900 (9th Cir. 2009)); *see also Gilday v. Dubois*, 124 F.3d 277, 296 n.27 (1st Cir. 1997) (analogizing "call detailing," which identifies the caller, the number called, and the date, time, and length of the call, to routing and signaling information associated with pen registers, and finding it outside the domain of the Electronic Communications Privacy Act). Instead, the *In re Apple* court analyzed whether the collected data were content by determining whether the information collected was what the user intended to communicate, like "words spoken in a phone call." *Id*. Because the data were automatically generated, "rather than through the intent of the user, [it could] not constitute content susceptible to interception." *Id*.

This description perfectly fits the data here. AdTech software does not capture substantive communications. It captures data about website activity, which is closely analogous to telephone call data, GPS tracking data, data about site visits, or non-audio surveillance, all of which have been held to be outside the scope of communications covered by the Wiretap Act. *See*, *e.g.*, *Com. v. Connolly*, 454 Mass.

808, 825 (2009) ("Data from GPS devices also does not fall within the language of the wiretap statute, G.L. c. 272, § 99 I 2, which authorizes interception of 'oral or wire communications.'"); *Com. v. Rousseau,* 465 Mass. 372, 378 n.9 (2013) (finding defendant's possible challenge of GPS warrant based on the Wiretap Act unavailing because GPS data were not subject to the statute). Thus, this Court should not view the data as "content" under the Wiretap Act's definition.

### B. The Tracked Information is Not an "Interception" Because Internet Users Have Notice the Information is Tracked

Under the Wiretap Act, for a recording to be "intercepted," the interception needs to be done secretly. In other words, if the fact that information is being tracked is not secret, the Wiretap Act is not applicable. G.L. c. 272, § 99(B)(4). This requirement precludes Plaintiffs' attempt to apply the Wiretap Act to the use of AdTech tracking, a ubiquitous technology that has been openly in use across the internet for more than two decades. The widespread use and existence of this technology is common knowledge for those with an understanding of how the internet works. It is routinely described in privacy policies and cookie warnings throughout the internet. Anyone who has ever browsed the internet cannot help noticing their browsing activity results in targeted advertising related to that activity. Indeed, to address this concern, every major browser offers a privacy or "incognito" mode to allow users to navigate the web without being tracked. The open nature with which this widespread technology is used on the internet precludes a finding

that the alleged interception is being done secretly. *See Com. v. Hyde*, 434 Mass. 594 (2001) (holding that if defendant had informed police of intention to record or "held the tape recorder in plain sight," there would be no violation of the Wiretap Act because recording would not have been secret); *Com. v. Jackson*, 370 Mass. 502, 507 (1976) ("We need not reach the question whether there was 'prior authority,' for such a consideration arises only if there is a finding that the conversations were recorded secretly."). Plaintiffs' attempt to elide this inconvenient statutory requirement by creating out of thin air a requirement that the disclosures be more obtrusive or contain some specific wording is without foundation.

## III. Imposing Liability Under the Wiretap Act for Use of Internet Tracking Technology Violates Due Process Rights and the Rule of Lenity

Though the question presented today is in the context of a civil dispute, the Wiretap Act is primarily a criminal statute. As a result, a finding that the Wiretap Act applies to the use of a technology routinely employed by thousands of websites in the Commonwealth would mean thousands of organizations and individuals could be criminally prosecuted for activities that they had no way of knowing was illegal. "Due process requires that 'laws give the person of ordinary intelligence a reasonable opportunity to know what is prohibited.'" *Upton v. S.E.C.*, 75 F.3d 92 (2d Cir. 1996) (quoting *Grayned v. City of Rockford*, 408 U.S. 104, 108 (1972)). "When a person of ordinary intelligence has not received fair notice that his contemplated conduct is forbidden, prosecution for such conduct deprives him of

due process." *United States v. Matthews*, 787 F.2d 38, 49 (2d Cir. 1986) (citations omitted).

### A. The Fair Warning Doctrine Prohibits Plaintiffs' Broad Interpretation of the Wiretap Act

Fair warning is analyzed through three related doctrines: vagueness, lenity, and unforeseeably expansive interpretation. "First, the vagueness doctrine bars enforcement of 'a statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application.'" *United States v. Lanier*, 520 U.S. 259, 266 (1997) (quoting *Connally v. General Constr. Co.*, 269 U.S. 385, 391 (1926)). A statute is unconstitutionally vague as applied when it "prohibits ... an act in terms so uncertain that persons of average intelligence would have no choice but to guess at its meaning and modes of application." *United States v. Hussein*, 351 F.3d 9, 14 (1st Cir. 2003). Due process requires that ambiguity in a statute be construed against criminal liability, in accordance with the rule of lenity. *Lanier*, 520 U.S. at 266. *See also Com. v. Rossetti*, 489 Mass. 589, 599 (2022) ("The rule of lenity requires us to give a defendant the benefit of any rational doubt where we conclude that a statute is ambiguous or we are unable to ascertain the intent of the Legislature."). "If the legislative history fails to clarify the statutory language, [the] rule of lenity would compel [the court] to construe the statute in favor of [defendants]." *Dixson v. United States*, 465 U.S. 482, 491 (1984). The doctrine reflects courts' deference to the

Legislature, the body "which possesses the power to define crimes and their punishment." *Lanier*, 520 U.S. at 265 n.5.

Lastly, "although clarity at the requisite level may be supplied by judicial gloss on an otherwise uncertain statute, due process bars courts from applying a novel construction of a criminal statute to conduct that neither the statute nor any prior judicial decision has fairly disclosed to be within its scope." *Lanier*, 520 U.S. at 266-267 (citations omitted). In sum, the doctrine bars "unforeseeable and retroactive judicial expansion of narrow and precise statutory language." *Bouie v. City of Columbia,* 378 U.S. 347, 352 (1964). Application of the statute to ubiquitous technology used throughout the Commonwealth would result in just such an unforeseeably expansive interpretation. The statute's three-year statute of limitations makes this problem even worse. If the Plaintiffs' interpretation of the statute were to hold, companies and individuals throughout the Commonwealth would be subject to criminal liability even if they stopped using AdTech tomorrow, since they cannot now cure the newly illegal behavior that occurred in the prior 36 months.

A person of ordinary intelligence would not have known that the widespread, widely publicized, and long standing[2] use of internet tracking technology violates a law from 1968 regulating the secret recording of telephone calls. Given the decades-long use of internet tracking technology, retroactive criminalization of a common internet business practice through a novel interpretation of a fifty-five-year-old statute is a clear due process violation.

### B. Applying the Wiretap Act to Internet Tracking Technology Would Harm Only Massachusetts Organizations

Application of the Wiretap Act to cover these internet tracking technologies would severely and unfairly prejudice Massachusetts-based organizations because the Wiretap Act does not by its terms apply to recordings conducted outside the Commonwealth, even if part of the interaction occurred inside the Commonwealth. *Marquis v. Google, Inc.*, No. 11-2808, 2015 WL 13037257, at *7 (Mass. Super. Feb. 13, 2015) ("nothing in the wiretap statute suggests any intention to regulate conduct outside the bounds of the Commonwealth.") (Citations omitted). In *Marquis*, the plaintiff alleged that Google scanned the content of emails sent or received by Gmail users for targeted advertising purposes. *Id.* at *1. Plaintiff used an AOL account

[2] *See*, *e.g.*, Tim Jackson, This bug in your PC is a smart cookie, FINANCIAL TIMES, February 1996, at 15; John Schwartz, Giving Web a Memory Cost Its Users Privacy, THE NEW YORK TIMES (Sept. 4, 2001), https://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html.

but sent emails to and received emails from Gmail accounts that resided on Google's servers located outside of Massachusetts, where the emails were then scanned. *Id.* at *2. The Superior Court found that Google had not violated the Wiretap Act because the interception occurred outside the Commonwealth and the Legislature likely did not intend for the Wiretap Act to apply to out-of-state conduct. *Id.* at *9. The court further held that "[a]pplying the Massachusetts wiretap statute to Gmail communications sent to or from a Massachusetts resident or visitor -- irrespective of where they might be scanned or processed -- would thus make compliance a game of chance" since emails can be sent or received anywhere with an internet connection. *Id.* at *8.

More recently in *Alves v. Goodyear Tire and Rubber Co.*, the U.S. District Court for the District of Massachusetts dismissed a putative class action against an out-of-state business involving allegations that were otherwise very similar to those presented here for lack of personal jurisdiction. No. CV 22-11820-WGY, 2023 WL 4706585 (D. Mass. July 24, 2023), *appeal dismissed*, No. 23-1682, 2023 WL 9782813 (1st Cir. Dec. 18, 2023). In *Alves*, Goodyear was alleged to have used Microsoft tracking technology to record Massachusetts residents' interactions with its website. The court held that because both Goodyear and Microsoft were domiciled outside Massachusetts, it was reasonable to infer that the interception took

place outside of Massachusetts, and therefore outside the bounds of the Wiretap Act. *Id*.

In light of *Marquis* and *Alves*, it is easy to see how the Plaintiffs' interpretation of the statute would lead to an unfair and anomalous result. One of Goodyear's competitors in Massachusetts is Sullivan Tire, a company headquartered in the Commonwealth. Under the Plaintiffs' interpretation of the Wiretap Act, if Goodyear and Sullivan Tire were to engage in exactly the same conduct and track Massachusetts citizens in exactly the same way while providing identical disclosures (or none at all), Sullivan Tire might be subject to ruinous civil liability and potential criminal conviction while Goodyear would be completely free from any criminal or civil liability.

Another consequence of this broad interpretation is the financial impact it will have on Massachusetts for-profit and nonprofit businesses. The charitable immunity statute does not limit the recovery of attorneys' fees awarded under the Wiretap Act. *Birbiglia v. St. Vincent Hosp., Inc.*, 427 Mass. 80 (1998). In *Birbiglia*, the trial judge reduced the damages on the wiretap count to $20,000, but allowed approximately $43,500 in attorney fees and costs, a form of relief that was expressly not subject to the $20,000 limit. *Id*. at 88. Now, almost 30 years later, a nonprofit hospital that was sued under the Plaintiffs' theory of liability paid almost $4.3 million in plaintiffs' attorneys' fees and costs while the named plaintiffs to the class action only

received $3,500 each. *Doe v. Partners Healthcare Sys., Inc.*, No. 1984CV01651-BLS-1 (Mass. Super. Ct.) (Dkt. No. 76). The result of finding for the Plaintiffs here will be to allow Massachusetts businesses to become financial targets for plaintiffs' attorneys, while boosting out-of-state businesses who will not be subject to what amounts to an unexpected and unintended tax for being a Massachusetts business.

Plaintiffs assert that this inevitable flood of litigation is imaginary by claiming that their lawsuits are targeted only at those few Massachusetts organizations that had inadequate disclosures for their use of AdTech software. But in the absence of any clarity on what constitutes "adequate" notice of AdTech -- which Plaintiffs have not tried to define, and for which there is no case law, rule, or regulation -- nothing will stop this wave of litigation crashing over Massachusetts businesses. Even if courts were now to define what constitutes adequate notice, this would not protect Massachusetts businesses from being sued for their allegedly incomplete notices during the course of the past three years. And even if the statute really only applied to a subset of Massachusetts businesses based on the sufficiency of their disclosures, that would not address the fact that Massachusetts businesses alone will be subject to this requirement, while their out-of-state competitors who engage in exactly the same conduct in the Commonwealth are exempt, a result that the Legislature could not have intended.

The unfairness of the Plaintiffs' statutory interpretation is further highlighted by the fact that Plaintiffs do not even allege any actual harm resulting from the alleged violation of the Wiretap Act. Their recovery calculation is based entirely on statutory damages, an amount likely to reach millions of dollars per website owner per year. Given that almost every citizen and business uses the internet, this would mean that virtually every person in Massachusetts could initiate a class action against virtually every business located in Massachusetts and be all but guaranteed an enormous recovery for the class (though the individual recoveries will be nominal). This cannot have been the Legislature's intent.

The Legislature may choose to regulate the nationwide AdTech business in Massachusetts, and if so, it can pass a law to do just that. In the absence of legislative action, however, it is not appropriate for courts to enable litigants to use an overbroad reading of the 1968 Wiretap Act as a means of regulating AdTech unevenly, unfairly, and retroactively.

## CONCLUSION

For these reasons, the Greater Boston Chamber of Commerce and the Massachusetts Nonprofit Network respectfully urge the Court to find in favor of Defendants Beth Israel Deaconess Medical Center, Inc. and New England Baptist Hospital, reverse the Superior Court's denials of their motions to dismiss, and direct the Superior Court to grant both motions with prejudice.

March 13, 2024

Respectfully submitted,

*/s/ Seth P. Berman*

Ian D. Roffman (BBO# 637564)
Seth P. Berman (BBO# 629332)
Natalie M. Cappellazzo (BBO# 699355)
Natalia Peña (BBO# 707596)
Nutter McClennen & Fish LLP
155 Seaport Boulevard
Boston, MA 02210
617-439-2000

*Attorneys for the Greater Boston Chamber of Commerce*

*/s/ Elka T. Sachs*

Elka T. Sachs (BBO# 562007)
ets@kb-law.com
Krokidas & Bluestein LLP
600 Atlantic Avenue, 19th Floor
Boston, MA 02210
617-482-7211

*Attorney for the Massachusetts Nonprofit Network*

**CERTIFICATE OF COMPLIANCE**
**Pursuant to Rule 16(k) of the**
**Massachusetts Rules of Appellate Procedure**

I, hereby certify that the foregoing brief complies with the rules of court that pertain to the filing of briefs, including, but not limited to:

Mass. R. A. P. 16 (a)(13) (addendum);
Mass. R. A. P. 16 (e) (references to the record);
Mass. R. A. P. 18 (appendix to the briefs);
Mass. R. A. P. 20 (form and length of briefs, appendices, and other documents); and
Mass. R. A. P. 21 (redaction).

I further certify that the foregoing brief complies with the applicable length limitation in Mass. R. A. P. 20 because it is produced in the proportional font Times New Roman at size 14, and contains 6,150, total non-excluded words as counted using the word count feature of Microsoft 365.

*/s/ Seth P. Berman*

Ian D. Roffman (BBO# 637564)
Seth P. Berman (BBO# 629332)
Natalie M. Cappellazzo (BBO# 699355)
Natalia Peña (BBO# 707596)
Nutter McClennen & Fish LLP
155 Seaport Boulevard
Boston, MA 02210
617-439-2000

March 13, 2024

## CERTIFICATE OF SERVICE

Pursuant to Mass.R.A.P. 13(d), I hereby certify, under the penalties of perjury, that on March 13, 2024, I have made service of this Amicus Brief upon all opposing parties and/or counsel of record for each party, by the Tyler Host System.

Edward F. Haber
Michelle H. Blauner
Patrick J. Vallely
SHAPIRO HABER & URMY LLP
ehaber@shulaw.com
mblauner@shulaw.com
pvallely@shulaw.com

David Quinn Gacioch
MCDERMOTT WILL & EMERY LLP
200 Clarendon Street, Floor 58
Boston, MA 02116
(617) 535-4000
dgacioch@mwe.com

*/s/ Seth P. Berman*
Ian D. Roffman (BBO# 637564)
Seth P. Berman (BBO# 629332)
Natalie M. Cappellazzo (BBO# 699355)
Natalia Peña (BBO# 707596)
Nutter McClennen & Fish LLP
155 Seaport Boulevard
Boston, MA 02210
617-439-2000

6533406