

COMMONWEALTH OF MASSACHUSETTS
THE 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

DEFENDANTS-APPELLANTS' AMENDED¹ OPENING BRIEF

Date: February 7, 2024

David Quinn Gacioch, BBO No. 660784
Annabel Rodriguez, BBO No. 696001
McDERMOTT WILL & EMERY LLP
200 Clarendon Street, Floor 58
Boston, MA 02116
(617) 535-4000
dgacioch@mwe.com
anrodriguez@mwe.com

¹ Amended pursuant to Mass. R. App. P. 11(g)(2) after the Court granted direct appellate review.

CORPORATE DISCLOSURE STATEMENT

Defendants-Appellants New England Baptist Hospital (“NEBH”) and Beth Israel Deaconess Medical Center, Inc. (“BIDMC”) (together, the “Hospitals”) are both Massachusetts non-profit corporations and public charities. Beth Israel Lahey Health, Inc., another Massachusetts non-profit corporation and public charity, is the sole corporate member and ultimate parent of both.

TABLE OF CONTENTS

CORPORATE DISCLOSURE STATEMENT2

ISSUES PRESENTED FOR REVIEW9

STATEMENT OF THE CASE.....11

STATEMENT OF FACTS13

SUMMARY OF ARGUMENT17

ARGUMENT18

I. Given the Act’s Criminal Provisions, the Rule of Lenity Requires that Every Statutory Ambiguity Be Resolved in the Hospitals’ Favor.20

II. Plaintiff Seeks Exactly the Type of Absurd, Unreasonable Outcome that Courts Consistently Avoid.....26

III. Website Browsing Actions Are Not “Wire Communications.”34

IV. No Secret Hearing or Recording Took Place, So No “Interception” Occurred.....39

V. The Wiretap Act Exempts from Liability Activities Undertaken In the Ordinary Course of Business, Using Standard Equipment.45

VI. Plaintiff’s Complaint Must Be Dismissed for Lack of Standing.52

CONCLUSION.....57

TABLE OF AUTHORITIES

	Page(s)
Cases	
<u>Alves v. BJ’s Wholesale Club, Inc.</u> , No. 2284CV02509-BLS1 (Suffolk Super. Ct.) (Mem. & Order, Dkt. No. 16, dated June 22, 2023)	12
<u>Anderson v. Nat’l Union Fire Ins. Co.</u> , 476 Mass. 377 (2017)	21
<u>Beard Motors, Inc. v. Toyota Motor Distribs., Inc.</u> , 395 Mass. 428 (1985)	55
<u>Matter of Chapman</u> , 482 Mass. 1012 (2019)	52
<u>Commonwealth v. Alleyne</u> , 474 Mass. 771 (2016)	40
<u>Commonwealth v. Ashford</u> , 486 Mass. 450 (2020)	21
<u>Commonwealth v. Boyarsky</u> , 452 Mass. 700 (2008)	40
<u>Commonwealth v. Byrd</u> , 661 Pa. 85 (2020)	44
<u>Commonwealth v. Connolly</u> , 454 Mass. 808 (2009)	37
<u>Commonwealth v. Ennis</u> , 439 Mass. 64 (2003)	26
<u>Commonwealth v. Guardado</u> , 491 Mass. 666 (2023) (vacated in part on other grounds)	43
<u>Commonwealth v. Jackson</u> , 370 Mass. 502 (1976)	43, 44, 45

<u>Commonwealth v. Luna,</u> 418 Mass. 749 (1994)	26
<u>Commonwealth v. Maccini,</u> Mass. Super. Ct., No. 06-0873, 2007 WL 1203560 (Apr. 23, 2007)	37, 44
<u>Commonwealth v. McCarthy,</u> 484 Mass. 493 (2020)	33
<u>Commonwealth v. McNeil,</u> 492 Mass. 336 (2023)	18
<u>Commonwealth v. Moody,</u> 466 Mass. 196 (2013)	<i>passim</i>
<u>Commonwealth v. Morganti,</u> 455 Mass. 388 (2009)	40
<u>Commonwealth v. Qasim Q.,</u> 491 Mass. 650 (2023)	26
<u>Commonwealth v. Wassilie,</u> 482 Mass. 562 (2019)	18
<u>Crosland v. Horgan,</u> 401 Mass. 271 (1987)	47
<u>Curtatone v. Barstool Sports, Inc.,</u> 487 Mass. 655 (2021)	<i>passim</i>
<u>Curtis v. Herb Chambers I-95, Inc.,</u> 458 Mass. 674 (2011)	20
<u>DiMasi v. Sec’y of the Commonwealth,</u> 491 Mass. 186 (2023)	18
<u>Doe v. Boston Med. Ctr. Corp.,</u> No. 2384CV00326-BLS1 (Suffolk Super. Ct.) (Mem. & Order, Dkt. No. 18, dated Sept. 15, 2023)	12, 38, 54
<u>Doe v. Boston Medical Center Corp.,</u> 2384CV00326-BLS1, slip op.	37

<u>Doe v. Children’s Hospital Corp.,</u> 2384CV00411-BLS1, slip op.	37, 38, 39
<u>Doe v. Emerson Hosp.,</u> No. 2277CV01000 (Essex Super. Ct.) (Mem. & Order, Dkt. No. 37, dated Nov. 22, 2023).....	12
<u>Doe v. Partners Healthcare Sys., Inc.,</u> No. 1984CV01651-BLS-1 (Mass. Super. Ct.).....	12
<u>Enos v. Secretary of Env’t. Affairs,</u> 432 Mass. 132 (2000)	53
<u>Ginther v. Comm’r of Ins.,</u> 427 Mass. 319 (1998)	52
<u>Harvard Crimson, Inc. v. President and Fellows of Harvard College,</u> 445 Mass. 745 (2006)	18
<u>Hershenow v. Enterprise Rent-A-Car Co. of Boston,</u> 445 Mass. 790 (2006)	54
<u>HSBC Bank USA, N.A. v. Matt,</u> 464 Mass. 193 (2013)	53
<u>J.M. v. C.G.,</u> 492 Mass. 459 (2023)	27
<u>Kenn v. Eascare, LLC,</u> No. 22-P-1017, 2024 WL 72736 (Mass. App. Ct. Jan. 8, 2024).....	55
<u>Kligler v. Attorney General,</u> 491 Mass. 38 (2022)	43, 56
<u>Leocal v. Ashcroft,</u> 543 U.S. 1 (2004).....	21
<u>Malloy v. Dep’t of Correction,</u> 487 Mass. 482 (2021)	27
<u>Marquis v. Google, Inc.,</u> Mass. Super. Ct., No. SUCV2011–02808–BLS1, 2015 WL 13037257 (Feb. 13, 2015).....	33

<u>Martin v. Gross,</u> 340 F.Supp.3d 87 (D. Mass. 2018) (reversed in part on other grounds)	37
<u>O’Sullivan v. NYNEX Corp.,</u> 426 Mass. 261 (1997)	33, 47, 51
<u>Pine v. Rust,</u> 404 Mass. 411 (1989)	<i>passim</i>
<u>Pishev v. City of Somerville,</u> 95 Mass. App. Ct. 678 (2019).....	55
<u>Pugsley v. Police Dep’t of Boston,</u> 472 Mass. 367 (2015)	52, 53
<u>Randolph v. Commonwealth,</u> 488 Mass. 1 (2021)	18
<u>Rich v. Rich,</u> Mass. Super. Ct., No. BRCV200701538, 2011 WL 3672059 (July 8, 2011)	37
<u>Shepard’s Pharmacy, Inc. v. Stop & Shop Cos., Inc.,</u> 37 Mass. App. Ct. 516 (1994).....	32
<u>State Bd. of Retirement v. Bulger,</u> 446 Mass. 169 (2006)	21
<u>State v. Lott,</u> 152 N.H. 436 (2005)	44
<u>Sudbury v. Mass. Bay Transp. Auth.,</u> 485 Mass. 774 (2020)	13
<u>TransUnion, LLC v. Ramirez,</u> 594 U.S. 413 (2021).....	55
<u>Velazquez v. Commonwealth,</u> 491 Mass. 279 (2023)	21

Statutes

G.L. c. 32, § 15(4).....21
G.L. c. 93A, § 9.....32, 33
G.L. c. 93H, § 1.....15
G.L. c. 272, § 99.....*passim*
G.L. c. 214, § 1B.....32, 33
Mass. R. Civ. P. 64(a).....11

Other Authorities

Webster’s 3d New Int’l Dictionary of the English Language –
Unabridged, at 460 (1968).....36

ISSUES PRESENTED FOR REVIEW

In this consolidated appeal,² the Hospitals raise the following issues of law:

- a. Whether an individual's browsing of a publicly-available website generates one or more "wire communications" under the Massachusetts Wiretap Act (the "Wiretap Act" or the "Act"), G.L. c. 272, § 99(B)(1), when such browsing activity does *not* include the sending or receipt of any email/text/chat/instant message or equivalent.

- b. *If so*, whether such a "wire communication" can be "intercepted" under the Wiretap Act (*i.e.* "secretly heard" or "secretly recorded"), see G.L. c. 272, § 99(B)(4), when the website user had actual or constructive knowledge that her browsing actions were being logged by one or more parties (e.g., the website owner, host, and/or operator), but she allegedly lacked knowledge that additional parties might receive data about her browsing actions.

² The two underlying cases are nearly identical. Plaintiff Kathleen Vita, represented by Shapiro Haber & Urmy LLP, brought both. NEBH and BIDMC are part of the same health system and are both represented by McDermott Will & Emery LLP.

- c. *If* the Massachusetts Wiretap Act is broad enough to cover technology that logs or shares data regarding users' browsing actions on public websites, as Plaintiff claims, whether the Act's exceptions for activities conducted in the ordinary course of business, see, e.g., G.L. c. 272, § 99(B)(3), must be construed equally broadly, rather than strictly limited to activities employing "any telephone or telegraph instrument, equipment, facility, or a component thereof" (narrowly defined), in order to preserve the careful balance the General Court struck when it drafted the Act in 1968 (when all wire communications traveled over telephone/telegraph wires and website technology did not exist) and to avoid absurd, unreasonable results.
- d. Whether a plausibly alleged violation of the Wiretap Act is alone sufficient to confer standing under Massachusetts law, even without any indication that a plaintiff has suffered any actual, direct, concrete, non-speculative, and imminent injury caused by a defendant's alleged acts.

The Hospitals properly preserved these issues at the Superior Court through briefing and oral argument on their motions to dismiss.

STATEMENT OF THE CASE

These are two among at least two dozen putative class action lawsuits that plaintiffs' lawyers have recently commenced against Massachusetts hospitals and other organizations, seeking to weaponize the Wiretap Act to create massive liability for website owners arising from website analytics and advertising technologies ("AdTech") that are ubiquitous in the 2020s. Plaintiff Kathleen Vita filed her complaint against BIDMC in Suffolk Superior Court's Business Litigation Session on February 24, 2023. R:A:I:6,8-57.³ She filed a nearly-identical complaint against NEBH in the same session on April 7, 2023. R:A:IV:6,9-52. Each alleges a single claim: violations of the Wiretap Act.

BIDMC moved to dismiss Plaintiff's complaint on June 9, 2023, and NEBH did so on June 22, 2023. R:A:I:61; R:A:IV:56. Plaintiff opposed both motions. R:A:I:100; R:A:II:95. After hearing combined oral argument, the Superior Court (Kazanjian, J.), on October 31, 2023, issued two Opinions and Orders, denying the motions to dismiss and simultaneously reporting its decisions to the Appeals Court for interlocutory appellate review, pursuant to Mass. R. Civ. P. 64(a). R:A:VII:65, 76. The resulting appeals were docketed on November 13, 2023. This Court granted the Hospitals' application for direct appellate review on January 17, 2024.

³ References to the Record Appendices appear as "R:A:[VOLUME NUMBER]:[PAGE NUMBER(S)]."

Plaintiffs' lawyers recently have filed hundreds of such opportunistic lawsuits around the country, targeting ubiquitous public website AdTech such as Google Analytics and Meta/Facebook Pixel. The first here in Massachusetts, against Partners Healthcare (now called Mass General Brigham) and Dana-Farber Cancer Institute, yielded an \$18.4 million settlement in 2022, after the Superior Court denied the defendants' motion to dismiss.⁴ At least twenty-four more such lawsuits then sprung up in quick succession, including these two.⁵ The Superior Court has now denied motions to dismiss in seven such cases,⁶ but this is the first appeal to address whether the Wiretap Act allows claims of this type. The Superior Court has stayed these two cases, and many of the others, pending disposition of this appeal.

⁴ See Doe v. Partners Healthcare Sys., Inc., No. 1984CV01651-BLS-1 (Mass. Super. Ct.) (Tr. of Rule 12 Hearing, dated Nov. 20, 2020 (R:A:II:32-119); Endorsed Order Allowing in Part and Denying in Part Motion to Dismiss, dated Dec. 7, 2020 (R:A:II:27)).

⁵ A list of all known cases alleging Wiretap Act violations based on public website AdTech is attached as Exhibit C to the Hospitals' application for direct appellate review, Vita v. New England Baptist Hospital, et al., DAR-29590 (SJC).

⁶ In addition to these two cases and Doe v. Partners, supra n.3, see Alves v. BJ's Wholesale Club, Inc., No. 2284CV02509-BLS1 (Suffolk Super. Ct.) (Mem. & Order, Dkt. No. 16, dated June 22, 2023); Doe v. Boston Med. Ctr. Corp., No. 2384CV00326-BLS1 (Suffolk Super. Ct.) (Mem. & Order, Dkt. No. 18, dated Sept. 15, 2023); Doe v. The Children's Hosp. Corp., No. 2384CV00411-BLS1 (Suffolk Super. Ct.) (Mem. & Order, Dkt. No. 18, dated Sept. 15, 2023); Doe v. Emerson Hosp., No. 2277CV01000 (Essex Super. Ct.) (Mem. & Order, Dkt. No. 37, dated Nov. 22, 2023).

STATEMENT OF FACTS⁷

Plaintiff alleges that each Hospital violated the Wiretap Act by “secretly” installing on its public website AdTech software provided by Google, Meta/Facebook, and other companies. R:A:I:8-9 & R:A:IV:9-10 (¶¶ 1-2). The Hospitals allegedly used AdTech for website optimization and marketing purposes. R:A:I:16, 53 (¶¶ 30,107); R:A:IV:16,46 (¶¶ 30,97). The software allegedly caused website visitors’ browsers (e.g., Google Chrome, Microsoft Edge, iOS Safari, etc.) to share certain information with the vendors (e.g., Google, Facebook, etc.) while those visitors browsed the Hospitals’ public websites. R:A:I:17-18 & R:A:IV:18-19 (¶¶ 38-39). Plaintiff alleges that AdTech typically logs and shares IP addresses and other computer attributes, along with 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. R:A:I:13,18,20,25-29 & R:A:IV:14-15,19,21-22,26-29 (¶¶ 22,39,49-50,61-68,71).

⁷ Because this appeal arose from denials of the Hospitals’ motions to dismiss, the factual record consists primarily of Plaintiff’s allegations. The Hospitals treat them as true for these purposes (only) but do not concede their accuracy. Plaintiff’s conclusory allegations of “secrecy”—or that “wire communications” or “interceptions” occurred, etc.—are not regarded as true even in this posture, because they are bare legal conclusions. See Sudbury v. Mass. Bay Transp. Auth., 485 Mass. 774, 778-79 (2020).

Notably, Plaintiff does *not* allege that anyone unlawfully obtained or shared any information about, or the content of, any email, text, instant, chat, or similar message that Plaintiff (or any other person) may have sent or received. Plaintiff also does *not* allege that any “interceptions” occurred within either Hospital’s patient portal (where patients can access medical records and other information specific to them, exchange messages with their providers, etc.) or any other access-restricted environment.⁸ Plaintiff alleges “interceptions” occurred only on the *publicly-available* portions of each Hospital’s website, and were limited to basic website browsing data (button/link clicks, URLs visited, words typed into form fields, etc.) generated by website visitors, who may or may not have been patients—as opposed to actual medical records or provider-patient communications.

Plaintiff asserts that the sensitivity (or lack thereof) of the “communication” or setting has no bearing on whether a Wiretap Act violation has occurred:

6. Although this case concerns the interception of communications that disclose healthcare consumers’ private health information, Plaintiff’s claim under the Massachusetts Wiretap Act does not depend on whether the intercepted communications reveal an individual’s private health information or any other sensitive information. *The Massachusetts Wiretap Act applies to all interceptions, regardless of the communication’s substance.*

⁸ Plaintiff’s complaints allege that AdTech operated on publicly-accessible pages of the Hospitals’ websites that contained *links* to the login pages of patient portal, medical records, and/or bill payment sites. R:A:I:46-51 (¶¶ 96-103); R:A:IV:38-47 (¶¶ 83-94). But Plaintiff does *not* allege that AdTech operated on those login pages or on any pages beyond them.

7. Moreover, although this case concerns communications between healthcare consumers and healthcare providers, ... [Plaintiff's Wiretap Act claim] ... does not depend on the nature of the relationship between Plaintiff and the Members of the Class and [the Hospital]. *The Massachusetts Wiretap Act applies to all interceptions, regardless of relationship, if any, among the parties to the communication.*⁹

Plaintiff alleges that the presence of AdTech was “secret,” but it is undisputed that each website displayed the following pop-up notice:¹⁰

We use cookies and other tools to enhance your experience on our website and to analyze our web traffic. For more information about these cookies and the data collected, please refer to our web privacy statement.

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 ...

R:A:I:13-14,92-93 & R:A:IV:14-15,87-88 (¶¶ 22-23; Ex. B) (emphases added).¹¹

⁹ R:A:I:10 & R:A:IV:11 (¶¶ 6-7) (emphases added).

¹⁰ R:A:I:14,92-93 & R:A:IV:15,87-88 (¶ 24 and Ex. B.)

¹¹ The privacy policy also included statements such as that the website “allows you to visit most areas without identifying yourself or providing personal information” and that at least some data gathered “is not shared with other organizations.” R:A:I:13-14 & R:A:IV:14-15 (¶¶ 22-23). Plaintiff argues that those statements were false and/or misleading, given the presence of AdTech—nullifying the disclosures. See id. Especially since G.L. c. 93H, § 1 defines “Personal Information” in a manner not implicated here (specifically requiring the presence of name plus, e.g., Social Security number, etc.), the Hospitals disagree.

Plaintiff makes almost no appearance in the factual allegations of her complaints. She alleges that she lives in Revere, that she is an NEBH patient, that her husband is a BIDMC patient, and that she “regularly uses” each Hospital’s website to “obtain information about [NEBH’s/BIDMC’s] doctors (including their credentials and backgrounds)” and to “search for information on particular [symptoms, conditions, and] medical procedures, [both for herself and her husband].” R:A:I:10-11 & R:A:IV:12 (¶ 10). She also alleges that she uses BIDMC’s website to “obtain and review her husband’s medical records through the website’s patient portal.” R:A:I:10-11 (¶ 10).¹² She alleges no other facts about herself or her own experience.

Neither complaint alleges that any actual harm or injury befell Plaintiff. In fact, she alleges nothing about the results of the purported “interceptions” beyond alleging that Google and Meta “can and do identify users on the website and associate their identities to the website users’ communications with the website ... [and] then use the communications to serve personalized advertising to those individuals.” R:A:I:13-14 & R:A:IV:14-15 (¶ 22). Plaintiff does not allege that *she* saw any such targeted advertising or that *anything* happened to her due to purported “interceptions.”

¹² As noted, Plaintiff does not actually allege that any AdTech operated within either Hospital’s patient portal.

SUMMARY OF ARGUMENT

In these two copy-and-paste lawsuits, Plaintiff argues that the Wiretap Act, overhauled in 1968, applies to public website AdTech that is ubiquitous in 2023—allowing website users to recover massive damages from each website owner whenever any AdTech is present and insufficiently disclosed. This attempted weaponization of the Act is far afield of the General Court’s intent in 1968, and it would expose thousands of Massachusetts businesses and non-profits to crippling civil liability, given the Act’s severe liquidated damages and fee-shifting provisions, as well as possible criminal prosecution. Both the rule of lenity (see pages 21-26 below) and the interpretive canon requiring avoidance of absurd and unreasonable results (pages 27-35) underscore that the Superior Court erred in accepting Plaintiff’s legal position.

Plaintiff cannot demonstrate that her website browsing actions constitute “wire communications” under the Act (pages 35-39). She cannot show that alleged logging of those browsing actions constituted “secret hearing” or “secret recording” under the Act (pages 40-46). She cannot avoid the fact that the General Court exempted activities conducted in the ordinary course of business, using standard equipment, from the Act’s prohibitions (pages 46-52). And she cannot establish standing, because she alleges no actual injury resulting from any purported violation (pages 53-57). The Superior Court erred in ruling otherwise. Reviewing *de novo*,

this Court should correct those errors of law and reverse the Superior Court’s denials of the Hospitals’ motions to dismiss.

ARGUMENT

These appeals turn on interpretation of the Wiretap Act. The goal of statutory interpretation is to “ascertain and effectuate” the General Court’s intent, consistent with “sound reason and common sense.”¹³ That work starts with the Act’s text, but does not end there. It is black letter law that Massachusetts courts will *not* adopt a construction of a statute—even a literal, textual one—that would lead to absurd or unreasonable results, because the General Court is presumed not to intend such results.¹⁴ But that is precisely what Plaintiff seeks: an interpretation of the Wiretap Act that would yield absurd and unreasonable results (a massive windfall of liquidated damages triggered by common business practices) that the General Court clearly could not have intended. As explained below, this Court can and should

¹³ Commonwealth v. Wassilie, 482 Mass. 562, 573 (2019); Harvard Crimson, Inc. v. President and Fellows of Harvard College, 445 Mass. 745, 749 (2006).

¹⁴ See, e.g., Commonwealth v. McNeil, 492 Mass. 336, 337 (2023) (“A fundamental tenet of statutory interpretation is that statutory language should be given effect consistent with its plain meaning and in light of the aim of the Legislature *unless to do so would achieve an illogical result.*”) (emphasis added) (quoting Sullivan v. Brookline, 435 Mass. 353, 360 (2001)); DiMasi v. Sec’y of the Commonwealth, 491 Mass. 186, 191-92 (2023) (“‘If the language is clear and unambiguous, it is conclusive as to the intent of the Legislature,’ ... and we enforce the plain wording *unless it would yield an absurd or unworkable result.*”) (emphasis added; citations omitted); Randolph v. Commonwealth, 488 Mass. 1, 6-7 (2021) (same).

interpret the Act’s text differently, in a manner consistent with common sense and legislative intent.

The Wiretap Act addresses warrantless “interception”—secret hearing or secret recording—of oral or wire communications using an “intercepting device.”¹⁵ The General Court rewrote the statute in 1968, with the clear intent to restrict people from secretly listening to or recording other peoples’ *interpersonal messages and conversations*. In 1968, interpersonal messages and conversations occurred in person, by telephone, by telegram (growing less common), or by letter. Federal law already prohibited the interception of mail. The General Court overhauled the Wiretap Act to cover the other three settings. The statute prohibited most surreptitious interceptions, created exceptions for commonplace activities that were *not* meant to be prohibited, and created detailed procedures governing interceptions by law enforcement.

Now, 55 years later, the Act still protects interpersonal conversations and messages from certain types of secret eavesdropping—even as those conversations and messages travel through new and different channels such as email, text messages, and videoconferencing. But these lawsuits attempt to stretch the Act far beyond what the General Court intended, or could possibly have imagined: to create

¹⁵ See G.L. c. 272, § 99(B),(C),(Q).

massive liability for ubiquitous AdTech that logs only browsing activity on public websites. This Court should reject those attempts because they fall far outside of the Act’s intended scope and are entirely inconsistent with fundamental canons of statutory interpretation.

In denying the Hospitals’ motions to dismiss, the Superior Court misinterpreted the Act. Given that posture and the nature of the issues raised, this Court’s review is entirely *de novo*.¹⁶

I. Given the Act’s Criminal Provisions, the Rule of Lenity Requires that Every Statutory Ambiguity Be Resolved in the Hospitals’ Favor.

The Wiretap Act is primarily criminal—defining multiple offenses punishable by incarceration before it reaches § 99(Q), under which Plaintiff sues. Those criminal offenses turn largely on the same elements and definitions as Plaintiff’s claims do here.¹⁷ Therefore, the rule of lenity *requires* that all plausible statutory ambiguities be resolved in the Hospitals’ favor.¹⁸ The U.S. Supreme Court has held that the rule of lenity applies to civil claims arising under statutory provisions that

¹⁶ See, e.g., Curtis v. Herb Chambers I-95, Inc., 458 Mass. 674, 676 (2011).

¹⁷ See G.L. c. 272, § 99(B),(C),(Q). Section 99(Q) also allows punitive damages, where (unlike here) the facts warrant them, drawing on the same elements. See Pine v. Rust, 404 Mass. 411, 415 (1989).

¹⁸ See Velazquez v. Commonwealth, 491 Mass. 279, 283 n.5 (2023) (“[W]here the language of a criminal statute plausibly can be found ambiguous, the rule of lenity *requires* that the defendant receive the benefit of the ambiguity.”) (emphasis added); accord, e.g., Commonwealth v. Ashford, 486 Mass. 450, 467 (2020).

also have criminal applications (to ensure consistent interpretation),¹⁹ and this Court has long applied the same concept to ambiguities in non-criminal, but nonetheless “penal,” Massachusetts statutes.²⁰

Here, the fundamental, case-dispositive statutory ambiguities that the rule of lenity requires be resolved in the Hospitals’ favor include:

1. whether the Act’s definition of “wire communication” reaches anything that is not an interpersonal message or conversation;
2. whether the Act’s “secrecy” element, which turns on the speaker’s actual or constructive knowledge, requires detailed, party-by-party knowledge/notice or only general knowledge/notice that *some* form of “recording” is taking place; and
3. whether the Act’s “ordinary course of business” exception is broad enough to cover 21st century technologies even though phrased in terms of “telephone or telegraph equipment.”

¹⁹ See Leocal v. Ashcroft, 543 U.S. 1, 11 n.8 (2004) (“[b]ecause we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context, the rule of lenity applies”).

²⁰ See, e.g., Anderson v. Nat’l Union Fire Ins. Co., 476 Mass. 377, 386 (2017) (applying rule of lenity to treble damages provisions of Chapter 93A); State Bd. of Retirement v. Bulger, 446 Mass. 169, 174-75 (2006) (“For purposes of statutory construction, G.L. c. 32, § 15(4), is considered to be penal and, therefore, its language *must* be construed narrowly, not stretched to accomplish an unexpressed result.”) (emphasis added).

The Hospitals raised the rule of lenity in their motions to dismiss, but the Superior Court did not address it.

To prevail on her Wiretap Act claims, Plaintiff must prove that at least one unlawful “interception” occurred, which the Act defines as “to secretly hear, secretly record, or aid another to secretly hear or secretly record the contents of any wire or oral communication through the use of any intercepting device.”²¹ In other words, Plaintiff’s claims cannot succeed without this Court accepting *every single one* of the following propositions:

- When a member of the public browses a publicly available website, her actions (e.g., scrolling, clicking links, entering URLs for desired webpages, etc.) constitute “wire communications” under the Act—even if they do not involve sending or receiving any email, text, chat, or instant message or the equivalent; *and*
- The act of digitally logging such browsing actions constitutes “hearing” and/or “recording” under the Act; *and*
- Ubiquitous AdTech software such as Google Analytics, Meta Pixel, etc. either (a) constitutes an “intercepting device” or (b) renders common

²¹ G.L. c. 272, §§ 99(B)(4),(B)(6),(Q).

digital hardware (e.g., servers, personal computers, tablets, smartphones, etc.) “intercepting devices” when installed; **and**

- Digital logging, using this ubiquitous software, is done in “secret”—*i.e.* without the website user’s actual knowledge and without sufficient notice to create constructive knowledge.

To accept all of those propositions, however, one must also accept several conclusions that ***necessarily*** follow from them:

1. Any “person”²² who willfully either:
 - a. engages in such logging using AdTech, or
 - b. attempts to do so, or
 - c. procures any other person to (attempt to) do so,commits a ***felony*** punishable by up to five years of imprisonment and a \$10,000 fine.²³
2. Any person who merely installs AdTech “under circumstances evincing an intent” to conduct logging creates *prima facie* evidence of guilt of that same ***felony*** offense.²⁴

²² Broadly defined as “any individual, partnership, association, joint stock company, trust, or corporation, whether or not any of the foregoing is an officer, agent or employee of the United States, a state, or a political subdivision of a state.” See G.L. c. 272, § 99(B)(13).

²³ See G.L. c. 272, § 99(C)(1).

²⁴ See id.

3. Any person who merely:
 - a. permits such logging activities to occur, or
 - b. “participates in a conspiracy” to engage in such activities, or
 - c. is an “accessory” to such activities,(*i.e.* anyone involved in deciding to use AdTech on a website or implementing that decision), is guilty of the same *felony* and punishable in the same manner.²⁵
4. Any person who willfully uses, or discloses to any other person, any such digital log, knowing its origin, commits a *misdemeanor* punishable by up to two years of imprisonment and a \$5,000 fine.²⁶
5. Any person who merely possesses AdTech software “under circumstances evincing an intent” to conduct logging also commits a *misdemeanor* punishable by up to two years of imprisonment and a \$5,000 fine.²⁷

There is no dispute that the AdTech about which Plaintiff complains is ubiquitous in 2023. It appears on the websites of most businesses, non-profit organizations, and government entities. Many thousands of people in Massachusetts

²⁵ See G.L. c. 272, § 99(C)(6).

²⁶ See G.L. c. 272, § 99(C)(3).

²⁷ See G.L. c. 272, § 99(C)(5).

have jobs that involve its creation, deployment, and usage. Thousands more supervise those individuals. Still thousands more have jobs in (*e.g.*, in marketing or communications, etc.) that make use of data derived from AdTech. In short, Plaintiff’s statutory construction would make presumptive criminals out of many thousands of Massachusetts residents—and not only for what they do going forward but also for multiple years of past conduct within the applicable statute(s) of limitations. The rule of lenity compels otherwise.

Plaintiff argues that the element of “willfulness” required for some of the criminal offenses detailed above solves this problem. She is wrong. First, not all of the offenses include a “willfulness” element.²⁸ Moreover, in this context and others, “willfully” just means “intentionally” rather than thoughtlessly or accidentally.²⁹ AdTech is often installed intentionally, not by accident. If the use of AdTech on a public website creates liability under § 99(Q), as Plaintiff argues, it most certainly creates criminal exposure under § 99(C).

²⁸ See G.L. c. 272, §§ 99(C)(5),(6).

²⁹ See, *e.g.*, Commonwealth v. Qasim Q., 491 Mass. 650, 658 (2023) (defining willfully as “intentional and by design in contrast to that which is thoughtless or accidental”); Commonwealth v. Ennis, 439 Mass. 64, 69 (2003) (applying similar definition in Wiretap Act context); Commonwealth v. Luna, 418 Mass. 749, 753 (1994) (“modern definition is that ‘wilful [sic] means intentional’ without making reference to any evil intent.”).

In sum, the rule of lenity *requires* the Court to resolve every relevant statutory ambiguity—of which there are several case-dispositive ones here—in the Hospitals’ favor. The Superior Court erred by not addressing and applying this interpretive canon to dismiss Plaintiff’s claims.

II. Plaintiff Seeks Exactly the Type of Absurd, Unreasonable Outcome that Courts Consistently Avoid.

A separate, and equally well-established, canon of statutory construction prevents absurd outcomes even when statutory text seems *unambiguous*.³⁰ This Court has long and consistently held that Massachusetts courts “will not adopt a construction of a statute that creates absurd or unreasonable consequences” when a reasonable, plausible alternative is available.³¹ But Plaintiff’s claims depend on the courts doing exactly that: interpreting the Wiretap Act in a manner that Plaintiff argues the text supports, but that would lead inexorably to absurd real-world outcomes. As explained below, other plausible interpretations of the Act are available that would *not* cause such unreasonable results, and they require dismissal of Plaintiff’s claims.

³⁰ See note 13, above.

³¹ J.M. v. C.G., 492 Mass. 459, 464 (2023) (quoting Lowery v. Klemm, 446 Mass. 572, 578-79 (2006)). Accord, e.g., Malloy v. Dep’t of Correction, 487 Mass. 482, 496 (2021) (quoting Att’y Gen. v. Sch. Comm. of Essex, 387 Mass. 326, 336 (1982)).

From shortly after its 1968 enactment, this Court and the Appeals Court have repeatedly declined to interpret the Wiretap Act out to the limits its text might arguably support. For example, in Commonwealth v. Todisco, a criminal defendant sought to exclude evidence of telephone conversations overheard by police officers during a search of the defendant's apartment, after the officers had repaired the apartment's telephones by replacing receiver units that had been removed.³² The defendant argued the replacement parts constituted intercepting devices.³³ This Court characterized the defendant's textual argument as "ingenious" but rejected it because it was "sustained neither by logic nor common sense."³⁴

Dillon v. Massachusetts Bay Transportation Authority is an even clearer example, which mirrors the present cases in many ways. There, a putative class of MBTA employees claimed Wiretap Act violations arising from the MBTA's allegedly-secret recording of telephone calls to and from its operations centers.³⁵ The Appeals Court affirmed summary judgment for the MBTA, citing the Act's "ordinary course of business" exception (addressed in detail below). The plaintiffs argued, based upon the Act's text, that the exception applied only to the use of

³² See 363 Mass. 445, 451-53 (1973).

³³ Id. at 452.

³⁴ Id.

³⁵ 49 Mass. App. Ct. 309, 310 (2000).

equipment obtained from a communications common carrier (the only source of standard telephone equipment in 1968), and that the MBTA’s recording equipment had been procured from a different source so it fell outside the exception.³⁶ The Appeals Court declined to follow the statutory text, prioritizing legislative intent and avoidance of absurd results—reasoning this Court later cited approvingly.³⁷

More recently, in Commonwealth v. Rainey, this Court denied a defendant’s motion to suppress audio-visual recordings of an alleged victim’s statement to police officers captured on a body-worn camera.³⁸ The Court expressly declined to apply the Act’s prohibitions as broadly as the text arguably might allow, quoting two past decisions for the proposition that, “[b]ecause we assume generally that the Legislature intends to act reasonably, we will not adopt a literal construction of a statute if the consequences of such a construction are absurd or unreasonable.”³⁹

The same approach is required here. Plaintiff’s attempt to overstretch the Act risks calamitous consequences across all for-profit and non-profit sectors of the Massachusetts economy—consequences the General Court could not possibly have

³⁶ Id. at 313-14.

³⁷ Commonwealth v. Moody, 466 Mass. 196, 207 (2013) (citing Dillon, 49 Mass. App. Ct. at 315).

³⁸ 491 Mass. 632, 642-44 (2023).

³⁹ Id. at 642-43 (quoting Commonwealth v. Diggs, 475 Mass. 79, 82 (2016); Champion v. Commonwealth, 422 Mass. 249, 251 (1996)).

intended. As detailed above (pages 14-15), Plaintiff admits her theory depends neither on the nature of any relationship between website owner and user nor on the sensitivity of any content allegedly “intercepted.”

Plaintiff’s theory applies no differently to non-profit hospital websites than it does to, for example:

- the menu page at dunkindonuts.com,
- the game schedule page at redsox.com,
- the “Exhibits” page on the Museum of Science’s website,
- the “Get Involved” page on the Greater Boston Food Bank’s website,
- the “Mass Times” page on the Roman Catholic Cathedral’s website,
- the “Summer Camp” page on Temple Israel of Boston’s website, and
- numerous pages on mass.gov,

to name just a few among millions of webpages that presently use AdTech just as the Hospitals’ websites allegedly did.

As the \$18.4 million Partners settlement shows, the magnitude of potential liability under the Act as applied to public website browsing in 2023 is *very different* from the 1968 context of discrete telephone calls and telegrams. The Act’s \$100 per day or \$1,000 per violation liquidated damages were designed for violations involving a discrete number of calls, telegrams, or in-person conversations, each involving two or perhaps a few participants—keeping multipliers within reason.

Here, Plaintiff argues that each website visitor whose browsing information is logged by AdTech generates another (minimum \$1,000) violation. Even for a small public website that gets just 1,000 unique visitors on an average day (light traffic, by website standards), Plaintiff's theory demands *at least \$36 million in damages per year*, over a three-year limitations period. And that's just for *one* lightly-used website—among many thousands across Massachusetts.^{40,41}

[intentionally blank for formatting reasons on next page]

⁴⁰ The Hospitals do not concede any aspect of Plaintiff's damages theory, including the applicable statute of limitations.

⁴¹ That is not the only absurdity in Plaintiff's approach. For example, it appears undisputed that the Hospitals did *not* violate the Wiretap Act themselves by logging Plaintiff's browsing actions on their own websites. Once validly created, nothing in the Act prevented the Hospitals from later forwarding such logs to third parties without notice to Plaintiff—just like nothing in the Act prevents one from forwarding an email without first advising the sender. Had the Hospitals allegedly forwarded their own logs to, e.g., Google, each night, rather than AdTech allegedly sharing certain browsing data in closer to real-time, there clearly would be no Wiretap Act claim. It is absurd and unreasonable that tens of millions of dollars of claimed liability could hang on such a minute and meaningless timing distinction.

The inherent absurdity is even clearer when one compares the Wiretap Act to the Commonwealth’s contemporaneous consumer/privacy protection statutes:

	Chapter 93A	Wiretap Act	Privacy Act⁴²
Enacted:	1967	1968	1974
Plaintiff must prove in order to recover:	<i>Both</i> statutory violation <i>and</i> resulting injury. ⁴³	Plaintiff here argues only a bare statutory violation (no resulting injury) required. ⁴⁴	Statutory violation and sufficient injury for standing to trigger nominal damages.
Damages available:	Actual damages (minimum \$25 per violation). ⁴⁶	Actual damages (<i>minimum \$1,000 per violation—40x the 93A amount</i>). ⁴⁷	Actual damages are available to the extent proven (no statutory minimum). ⁴⁵
A willful/ knowing violation triggers:	Treble damages (minimum \$75 per violation). ⁴⁸	<i>Felony prosecution</i> (up to five-year prison sentence and \$10,000 fine) and possibly punitive damages. ⁴⁹	Possibly punitive damages.

⁴² G.L. c. 214, § 1B.

⁴³ See G.L. c. 93A, § 9(1),(3).

⁴⁴ The Hospitals refute this argument below.

⁴⁵ See, e.g., Shepard’s Pharmacy, Inc. v. Stop & Shop Cos., Inc., 37 Mass. App. Ct. 516, 524 (1994) (reversing damage award that exceeded actual proven damages).

⁴⁶ See G.L. c. 93A, § 9(1),(3).

⁴⁷ See G.L. c. 272, § 99(Q).

⁴⁸ See G.L. c. 93A, § 9(3).

⁴⁹ See G.L. c. 272, § 99(C).

Given these stark contrasts, the General Court in 1968 clearly intended the Wiretap Act’s severe penalties to target only a very limited range of conduct that is both serious and unambiguously wrongful—conduct that is criminal if done by design. The consequences of violating the Act *far* exceed those of both Chapter 93A, which addresses unfair and deceptive business practices, and the Privacy Act, which was enacted for the explicit purpose of protecting individuals “against *unreasonable, substantial or serious* interference[s] with [their] privacy.”⁵⁰ The Wiretap Act obviously was *not* intended as a tool for policing ordinary business practices—even those alleged to be unfair, deceptive, or insufficiently privacy-protective—as Plaintiff attempts to do here.⁵¹

⁵⁰ G.L. c. 214, § 1B (emphasis added). See, e.g., Commonwealth v. McCarthy, 484 Mass. 493, 510 n.18 (2020) (Privacy Act was intended to “protect[] individuals from disclosure of facts ... that are of a highly personal or intimate nature when there exists no legitimate, countervailing interest.”) (cleaned up).

⁵¹ The Act’s lack of reference to class actions, unlike c. 93A, § 9(2), supports this conclusion. Before the Partners lawsuit in 2019, there were very few attempts to wield the Act broadly, targeting commercial conduct, and Massachusetts courts ultimately *rejected every one of them* (as far as undersigned counsel’s research indicates). See, e.g., O’Sullivan v. NYNEX Corp., 426 Mass. 261, 263, 266-67 (1997) (affirming summary judgment for NYNEX against customer claims); Dillon, 49 Mass. App. Ct. at 310, 319 (affirming summary judgment for the MBTA in putative employee class action); Marquis v. Google, Inc., Mass. Super. Ct., No. SUCV2011–02808–BLS1, 2015 WL 13037257, at *1, 9 (Feb. 13, 2015) (granting defendant’s motion for summary judgment on Gmail-based Wiretap Act claims) and 2014 WL 4180400, at *1, 16 (July 27, 2014) (denying plaintiff’s motion for class certification in same case).

Massachusetts courts do not interpret statutes in ways that defy common sense and yield absurd results. Yet that is exactly what Plaintiff's seeks here: to interpret the language of this pre-internet age statute in a way that creates unintended, absurd, and calamitous internet age consequences.

Plaintiff tries to sidestep this fatal flaw in her approach by arguing that the Hospitals overstate the consequences of a ruling in her favor. Plaintiff argues that avoiding liability is simple: a website owner must merely disclose the presence of AdTech. In theory, that sounds like a reasonable solution. In practice, it is anything but.

First, the Hospitals *did* disclose the collection of browsing data by themselves and at least one third party. They included a prominent banner notice to alert users. Nonetheless, Plaintiff contends that these disclosures were not clear or extensive enough, or were self-contradictory in part, so they are meaningless.

Second, the Hospitals are not outliers. Every major hospital in Massachusetts has been sued in this litigation wave, along with several others (health care providers, health insurers, retailers, etc.). Those more than two dozen defendants (and counting) employed varying degrees of disclosure on their websites, but plaintiffs' lawyers have deemed all efforts insufficient. They are making up the sufficiency standard as they go.

Third, Plaintiff’s “just disclose” solution does not address the massive *retrospective* liability her legal theory would create. It is not as if a new law regarding disclosure of AdTech will take effect in a few months and all website owners need only make sure they have compliant disclosures in place by that time. Instead, Plaintiff contends that the Wiretap Act *already* imposed the standard she espouses (and created substantial liability for anyone falling short of it). If this Court were to accept Plaintiff’s position, many thousands of Massachusetts organizations and individuals would face massive backward-looking exposure within the applicable limitations periods. In sum, Plaintiff’s “just disclose” argument does nothing to mitigate the absurd and unreasonable results that necessarily would follow from her legal theories. They must be rejected.

III. Website Browsing Actions Are Not “Wire Communications.”

To prevail, Plaintiff must prove that “wire communications” were unlawfully intercepted. The Act defines “wire communication” as “any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception.”⁵² It does not define “communication,” but its text and structure show the General Court meant messages or conversations between people.

⁵² G.L. c. 272, § 99(B)(1).

The Act mentions “telephone” seven times and “telegraph” five times, in contexts indicating that they constitute the entire universe of wire communication pathways the General Court had in mind.⁵³ It mentions no other wire communications pathways.

Telephone and telegraph inherently are means of interpersonal communication: one person speaks or writes a message and one or more persons listen to or read that message. Contemporaneous dictionary definitions of “communication(s)” and “wire” point in the same direction: to messages exchanged between people, often over telephone or telegraph wires (but listing no other types).⁵⁴

While courts have applied the Wiretap Act to wire communications technologies that did not exist in 1968, that has always been in the context of

⁵³ See G.L. c. 272, §§ 99(B)(3), (D)(1)(f), (F)(2)(c), (I)(3), (J)(1), (L)(1). For example, in listing the required contents of an eavesdropping warrant application, § 99(F)(2)(c) requires specification that “[t]hat the oral or wire communications of the particularly described person or persons will occur ... over particularly described *telephone or telegraph* lines.” (Emphasis added.) Subsections 99(J)(1) and (L)(1) similarly presume that any intercepted wire communications would travel over telephone/telegraph lines.

⁵⁴ See Webster’s 3d New Int’l Dictionary of the English Language – Unabridged, at 460 (1968) (defining “communications” as, e.g., “a system (*as of telephones or telegraphs*) for communicating information and orders (as in a naval service)” and “a process by which meanings are exchanged *between individuals* through a common system ...”); *id.* at 2623 (defining “wire” by reference to telegraph and telephone systems but no other communication pathways). (Emphases added.)

interpersonal communications—until this AdTech litigation began. Courts have applied the Act to emails and chat/instant messages,⁵⁵ but those are just the modern equivalents of the interpersonal telegrams the Act expressly covers.

Plaintiff’s purported “communications” here are very different. They are just movements in digital space—navigating and searching through public webpages just as one would physically navigate and search through library or bookstore aisles and shelves, seeking content created and published prior to one’s search, or just as one might physically approach the door of a store to check its posted hours of operation. The Act clearly does *not* apply to technology that monitors and records physical movements, such as video-only surveillance cameras or GPS devices.⁵⁶ Plaintiff’s attempt to apply the Act to digital movements must fail.

The Superior Court rejected this argument for reasons stated in its denials of motions to dismiss parallel complaints against Boston Medical Center and Boston Children’s Hospital.⁵⁷ There, the Superior Court described a 1991 dictionary

⁵⁵ See, e.g., Moody, 466 Mass. at 207-09; Rich v. Rich, Mass. Super. Ct., No. BRCV200701538, 2011 WL 3672059, at *4 (July 8, 2011); Commonwealth v. Maccini, Mass. Super. Ct., No. 06-0873, 2007 WL 1203560, at *3 (Apr. 23, 2007).

⁵⁶ See, e.g., Commonwealth v. Connolly, 454 Mass. 808, 825 (2009); Martin v. Gross, 340 F.Supp.3d 87, 92-93 (D. Mass. 2018) (reversed in part on other grounds).

⁵⁷ R:A:VII:92-94, 104 (Opinion & Order at 6, citing Doe v. Boston Medical Center Corp., 2384CV00326-BLS1, slip op. (“BMC Decision”) at 6-7 and Doe v. Children’s Hospital Corp., 2384CV00411-BLS1, slip op. (“BCH Decision”) at 4-6.)

definition of “communication” as “not limited to human-to-human speech or conversations, but, as common sense would dictate, include[ing] writing and signs.”⁵⁸ But that cannot define the (1968) Wiretap Act’s scope. If it did, one could violate the Act by photographing or video-only recording an electronic sign board or a vehicle’s turn signal (which rely in part on wires to convey visual messages).

The Superior Court also adopted plaintiffs’ argument that the Act “is to be interpreted broadly,” citing Moody.⁵⁹ While Moody states that *the General Court* chose to define the term “wire communication” “broadly,” the Moody Court had before it only the question of whether the term included mobile phone calls and text messages—direct successors to the interpersonal telephone calls and telegrams the Act expressly covers.⁶⁰ Moody says nothing about stretching the Act further than that. And Moody cannot stand for the proposition that the Act is to be *judicially interpreted* broadly overall, because that would directly conflict with the rule of lenity—an issue the Moody Court did not even mention.

The Superior Court reasoned that “[o]nline searches for doctors and requests for appointment [sic] also did not exist in 1968, but, similar to texting, are the modern equivalent of telephone inquiries and conversations with doctors’ offices

⁵⁸ R:A:VII:93 (BCH Decision at 5 (citing Webster’s Collegiate Dictionary 274 (1991))).

⁵⁹ R:A:VII:93-94 (BCH Decision at 5-6 (citing 466 Mass. at 209)).

⁶⁰ See 466 Mass. at 207-09.

that would have occurred then.”⁶¹ That reasoning proves far too much. If a library or bookstore (or even hospital lobby/waiting room) security camera recorded someone reading a printed physician directory or a “Boston’s Best Doctors” magazine issue, that obviously would not violate the Wiretap Act. Just because one *could* perform a task via telephone (e.g., calling a bookstore to ask whether a particular book is in stock), that doesn’t mean that the Wiretap Act covers *every* means of accomplishing the task—especially when some do *not* involve interpersonal conversations (e.g., visiting the bookstore to check the shelves).

Finally, the Superior Court noted that the Act’s preamble says nothing that would limit its intended reach to interpersonal conversations.⁶² Here again, given the Act’s criminal/penal nature, the rule of lenity requires courts to resolve open questions in *defendants’* favor, not in favor of expansive liability. The Superior Court erred in reversing that presumption.

⁶¹ R:A:VII:94 (BCH Decision at 6).

⁶² R:A:VII:104 (BMC Decision at 6).

IV. No Secret Hearing or Recording Took Place, So No “Interception” Occurred.

Plaintiff must also show that the complained-of “hearing” or “recording” occurred in “secret.” The relevant question is *not* whether Plaintiff *consented*.⁶³ Instead, it is whether Plaintiff had actual or constructive knowledge of the basic fact that “hearing” or “recording” was taking place.⁶⁴ Here, Plaintiff had sufficient notice of the “hearing” and “recording” of which she complains for at least two reasons: (1) common knowledge of how the internet and websites inherently work, and (2) the Hospitals’ specific disclosures to website users about data collection.

The Hospitals raised both points in their motions. The Superior Court addressed only the latter in its decisions, concluding that the Hospitals “disclose[d] the existence of only a *single* ‘Third Party Service Provider,’ while the Complaint alleges that the data [the Hospital] collects is contemporaneously shared with *multiple* external organizations (Google, Meta, and others)” so notice was insufficient.⁶⁵

⁶³ See Curtatone v. Barstool Sports, Inc., 487 Mass. 655, 658-59 (2021); Commonwealth v. Alleyne, 474 Mass. 771, 785 (2016); Commonwealth v. Morganti, 455 Mass. 388, 400-01 (2009); Commonwealth v. Boyarsky, 452 Mass. 700, 705 (2008).

⁶⁴ See, e.g., Curtatone, 487 Mass. at 658-59.

⁶⁵ R:A:VII:71,83 (Opinion & Order at 7 (emphases in original)).

In so doing, the Superior Court effectively adopted Plaintiff's theory that each and every "recording," and each and every party who might have access, must be disclosed in order to remove secrecy. This Court's precedent says the opposite.

In Curtatone, a Barstool Sports representative falsely claimed to be a *Boston Globe* reporter to obtain a telephone interview with Somerville Mayor Joseph Curtatone, who had previously declined to speak with Barstool.⁶⁶ The Barstool representative, posing as a *Globe* reporter, recorded the conversation (with the mayor's permission) and then posted the recording on Barstool's website.⁶⁷ Curtatone sued Barstool under § 99(Q), alleging unlawful interception because the interview and recording had been obtained through intentionally false pretenses: in essence, that Barstool had secretly heard/recorded the conversation because Curtatone understood that he was speaking only to the *Globe* and permitted only the *Globe* to record.⁶⁸ Barstool moved to dismiss. The Superior Court granted Barstool's motion and this Court unanimously affirmed.⁶⁹

This Court ruled that no unlawful interception occurred because the ***act of recording itself*** was not secret, even if the recorder's identity was intentionally kept

⁶⁶ 487 Mass. at 656-57.

⁶⁷ Id. at 657.

⁶⁸ Id. at 655-58.

⁶⁹ Id. at 656.

secret (indeed, falsified).⁷⁰ Curtatone knew *someone* was recording him. That was enough to prevent a violation, even though he was intentionally misled as to who that was and what they would do with the recording.

This Court ruled similarly twice in 2023. In Commonwealth v. Morris, police officers audio-visually recorded a suspect’s confession without informing him, and that recording was introduced at trial, resulting in a murder conviction.⁷¹ The Court unanimously affirmed the Superior Court’s decision not to suppress the recording. The majority reasoned that the defendant made a voluntary statement, which he understood officers were “recording” through handwritten notes, and the officers made vague comments about an eventual audience, so no violation occurred.⁷² And that was in the gravest possible circumstance—affirmation of a conviction that resulted in a life sentence.⁷³

In Rainey, the Court unanimously rejected a defendant’s argument that the introduction at his probation revocation proceeding of an audio-visual recording of a victim interview, captured by a police body-worn camera, had violated the Wiretap

⁷⁰ Id. at 659-60 (“The identity of the party recording the communication or, indeed, the truthfulness with which that identity was asserted is irrelevant; ***rather, it is the act of hearing or recording itself that must be concealed*** ...” to create a violation) (emphasis added).

⁷¹ 492 Mass. 498, 501-02 (2023).

⁷² Id. at 505-07.

⁷³ Id. at 502.

Act.⁷⁴ The victim had not known she was being audio-visually recorded, but she voluntarily made a statement to police officers, knowing that they were “recording” that statement by taking notes.⁷⁵ Thus, no violation had occurred.⁷⁶

In Curtatone, Rainey, and Morris, there was no Wiretap Act violation because the speaker had enough notice that *some* type of “recording” was occurring. The speaker did not have to know exactly what type of recording was occurring, or who specifically was recording, or with who else the recording might be shared.^{77,78}

⁷⁴ 491 Mass. at 633.

⁷⁵ Id. at 643-44.

⁷⁶ See id.

⁷⁷ The same was true in Commonwealth v. Jackson, 370 Mass. 502 (1976). The defendant’s offhand and general statements over the phone such as “I know the thing is being taped” were alone sufficient to prevent any Wiretap Act violation when audio recordings of the calls made by the victim’s brother were shared with law enforcement. Id. at 504, 507.

⁷⁸ Plaintiff may argue that a recent Appeals Court decision holds that, for a single communication, each additional audience for, or use of, a recording constitutes a separate interception if insufficiently disclosed. See Commonwealth v. Du, No. 22-P-870, 103 Mass. App. Ct. 483, at 17 (2023). To the extent Du so held, it did so without any basis in Wiretap Act jurisprudence. The Du court considered not a single prior Wiretap Act precedent. Moreover, any such aspect of Du was mere *dicta*—neither briefed by the parties nor necessary to resolve the appeal. See, e.g., Commonwealth v. Guardado, 491 Mass. 666, 692 (2023) (vacated in part on other grounds) (citing Commonwealth v. Mathews, 450 Mass. 858, 871 (2008) as “discounting dicta as precedent”); Kligler v. Attorney General, 491 Mass. 38, 71-72 (2022) (“Of course, the statement undoubtedly was dictum and therefore is not a controlling statement of law.”). With the benefit of actual briefing, the Appeals Court likely would have considered Wiretap Act precedents such as Curtatone, Rainey, Morris, and Jackson, and ruled differently. A petition for further appellate review is pending. (No. FAR-29556).

This Court’s consistent interpretation of the Act’s “secrecy” element shows that the Superior Court erred in denying the Hospitals’ motions. Plaintiff had sufficient notice of the basic fact of “recording,” both generally and specifically.

First, as a matter of law, Plaintiff had sufficient general notice of the alleged “recording.” It is common knowledge in the 2020s that websites cannot follow users’ browsing commands without logging (*i.e.*, “recording”) them. That is how the internet inherently works, as multiple courts in Massachusetts and elsewhere have recognized, in the context of internet-based *actual* communications such as emails and chat messages. More than fifteen years ago, Justice Fabricant explained that “[o]ne who uses [email or instant messaging] ... is on notice of the inherent recording, and implicitly consents to it.”⁷⁹ Plaintiff not only knew but *necessarily intended* that her “communications” with the Hospitals’ websites would be “recorded”—because the websites could not have displayed the content she sought without first logging her browsing actions.

Based on the holdings of Curtatone, Morris, Rainey, and Jackson, this general notice of inherent recording is, alone, sufficient to defeat secrecy—and for *all* purposes, not just for the Hospitals’ own data logging. Thus, Plaintiff’s claims fail

⁷⁹ See, e.g., Maccini, 2007 WL 1203560, at *3. Courts elsewhere have ruled similarly. See, e.g., Commonwealth v. Byrd, 661 Pa. 85, 99 (2020) (“[B]y the very act of sending a communication over the Internet, the party expressly consents to the recording of the message.”); State v. Lott, 152 N.H. 436, 439-42 (2005).

as a matter of law. The Superior Court erred in ruling otherwise (indeed, not addressing this general notice argument at all).

Second, each Hospital provided prominent, specific notice of data collection. As detailed above, each website displayed a pop-up notice to users, which linked to a fuller privacy policy. Together, they disclosed the collection of browsing data by the website owner and at least one “Third Party Service Provider.” These warnings were sufficient to eliminate any secrecy as a matter of law.

The Superior Court erred in rejecting this argument, due to the alleged lack of specificity of the Hospitals’ disclosures. Its reasoning would have required the police officers in Morris and Rainey to have detailed for the defendant (in Morris) or the victim (in Rainey) *both* that audio-visual recording was taking place *and* that the resulting recordings would be shared with each of the following parties: (a) other officers, (b) prosecutors, (c) defense counsel, (d) trial court judges or Parole Board members, (e) grand jurors and trial jurors (in Morris), etc., etc. The same would apply to Jackson.

The Superior Court’s reasoning would never have allowed dismissal of Curtatone’s claim against Barstool, given that Barstool obtained the interview in the first place through outright fraud. The Superior Court’s approach would have required the Barstool representative not only to identify himself accurately but also

to detail for Curtatone every other audience with whom the recording would be shared.

That is clearly not the law. The Superior Court erred.

V. The Wiretap Act Exempts from Liability Activities Undertaken In the Ordinary Course of Business, Using Standard Equipment.

The Superior Court also should have granted the Hospitals' motions because Plaintiff failed to plausibly allege the use of an "intercepting device."⁸⁰ Plaintiff contends that AdTech itself constitutes an intercepting device.⁸¹ But Plaintiff also alleges facts showing that any use of AdTech occurred in the ordinary course of the Hospitals' business (developing and operating their websites and marketing).⁸² That means the AdTech cannot be an intercepting device, as a matter of law.⁸³

The Act's "ordinary course of business" exception plays a key role in maintaining the intended legislative balance. It shows that the Act was meant to address surreptitious, unexpected, out-of-the-ordinary hearing or recording of

⁸⁰ See G.L. c. 272 § 99(B)(3).

⁸¹ R:A:I:55 (¶ 119); R:A:IV:50 (¶ 109).

⁸² See, e.g., R:A:I:15-18,52 (¶¶ 26-40,107) & R:A:IV:16-19,47 (¶¶ 26-40,97).

⁸³ See G.L. c. 272, § 99(B)(3) (excluding from definition of "intercepting device" "any telephone or telegraph instrument, equipment, facility, or a component thereof, (a) furnished to a subscriber or user by a communications common carrier in the ordinary course of its business under its tariff and being used by the subscriber or user in the ordinary course of its business; or (b) being used by a communications common carrier in the ordinary course of its business.")

interpersonal communications, not normal business operations (even if secret).⁸⁴ This Court and the Appeals Court have always applied the exception broadly and flexibly. Indeed, undersigned counsel’s research has *not uncovered a single instance* in which either court has considered the exception and ruled it did not apply.⁸⁵

The Dillon decision, which this Court cited approvingly in Moody, epitomizes that approach. There, as here, plaintiffs’ counsel pursued a class action for statutory damages under § 99(Q), the defendant argued that “interception” did not reach “ordinary course of business” measures, and the plaintiffs countered with a text-focused argument—that the exception applied only to equipment supplied by the phone company (a “communications common carrier”) and not to equipment procured from another source.⁸⁶ Both the Superior Court and the Appeals Court rejected that argument and ruled for the MBTA and a common sense interpretation.

⁸⁴ See also G.L. c. 272, § 99(A) (explaining legislative purpose as including prohibition of “the secret use of [surveillance] devices by private *individuals*” with no mention of businesses) (emphasis added).

⁸⁵ See O’Sullivan, 426 Mass. at 266-67 (defendant’s secret recordings of telemarketing calls made to subscribers fell within ordinary course of its business and, thus, did not violate the Act); Crosland v. Horgan, 401 Mass. 271, 276 (1987) (use of hospital’s telephone extension to secretly eavesdrop on call to bomb threat suspect, orchestrated by police detective, fell within hospital’s ordinary course of business because it was “reasonably related to a legitimate business purpose” and, thus, did violate the Act); Dillon, 49 Mass. App. Ct. at 319.

⁸⁶ 49 Mass. App. Ct. at 312-13.

The Appeals Court explained:

We do not depart lightly from the express wording of a statute ... but in the unusual circumstances appearing here we agree ... that a deviation is justified. The [Act’s amendment history] does not bar us from reading the exception so as to *preserve it in its intrinsic intended scope and maintain its viability in the broad run of cases; the plaintiffs' proposal would in effect destroy the exception.* Thus the decision below comports with the *canons that interpretation should tend to preserve the substance of a statute rather than diminish it ...; should not override common sense ...; or produce absurd or unreasonable results ...* — in this case *the absurdity of allowing the fortuity of the source of the equipment to entail serious material consequences.*⁸⁷

Plaintiff here urges a similar interpretation of 1968 text, with no regard for the absurd results that would follow in 2023. Plaintiff contends that the “ordinary course of business” exception applies only where “a telephone or telegraph instrument, equipment, facility, or a component thereof” (narrowly defined) is used, and that AdTech doesn’t qualify. But Dillon rejected such approaches that would “destroy the exception,” “override common sense,” and “produce absurd or unreasonable results.”⁸⁸ This Court should do the same here.

Plaintiff argues the General Court simultaneously created both (1) a prohibition against interceptions that was expansive and flexible enough to cover 21st century website technologies that were unimaginable in 1968 *and* (2) a counterbalancing “ordinary course of business” exception that was strictly limited

⁸⁷ Id. at 315-16 (citations omitted; emphases added). This Court approvingly quoted some that language in Moody. See 466 Mass. at 207.

⁸⁸ 49 Mass. App. Ct. at 315-16 (citations omitted).

to the use of “telephone or telegraph equipment” as that phrase would be understood in 1968. Plaintiff’s desired outcome is precisely what Dillon rejected: as technology and norms evolve over time, the exception gets smaller and smaller vis-à-vis the corresponding prohibition—“in effect destroy[ing] the exception” and throwing off the careful legislative balance, rather than preserving its “intrinsic intended scope.”

Moreover, Plaintiff’s approach requires the Court to hold that the General Court in 1968 created a robust exception *within its indisputable core area of concern* (secret eavesdropping on interpersonal telephone conversations) but did *not* intend that exception to apply in more peripheral—and then-unimaginable—applications of the Act (website browsing data). Per Plaintiff, in 2024, it is simultaneously:

- *lawful* for a business to secretly record and disseminate *voice calls* with its customers if done in the ordinary course, using traditional telephone equipment; but
- a potential *felony*, and a basis for crushing damages, for the same business to secretly “record” and disseminate, in the ordinary course, those same customers’ browsing actions on its public website—simply because different technology is used.

The further one travels from the General Court’s core concern, the *broader* Plaintiff argues the liability exposure gets. That would be absurd and Plaintiff offers no explanation for why the General Court could possibly have so intended.

The Superior Court here felt compelled by the lack of appellate law on the question to accept Plaintiff’s blindered approach. It ruled that the exception’s text requires “telephone or telegraph equipment” and that “the electronic software-based internet tracking technology at issue here plainly is not telephone or telegraph equipment.”⁸⁹ Citing a recent denial of a motion to dismiss a parallel case against BJ’s Wholesale Club, the Superior Court explained, “[f]or that reason, *in the absence of an appellate decision extending the exception beyond the realm of telephones and telegraphs*, under the plain language of the statute, the court declines to apply the exception here.”⁹⁰ And the Superior Court simultaneously reported its decisions for interlocutory review precisely to obtain such appellate guidance.

Traditional telephone and telegraph equipment were the only types of standard-issue equipment available in 1968 to hear or record a wire communication—because wire communications traveled over telephone and telegraph wires at that time. There is no common-sense or otherwise plausible explanation for why the General Court would have allowed one to legally undertake

⁸⁹ R:A:VII:72,84 (Opinion & Order at 8.)

⁹⁰ R:A:VII:72,84 (Opinion & Order at 8 (emphasis added)).

with traditional telephone or telegraph equipment an action that would be a felony, and the basis for substantial damages, if undertaken using some other standard, commercially-available technology.⁹¹ Allowing that unexplained distinction to have such “serious material consequences” would be just as absurd here as was a material distinction based on “the fortuity of the source of the equipment” in Dillon.⁹² It simply cannot be correct.

There is no plausible dispute about whether the Hospitals used AdTech in a manner “reasonably related to legitimate business purposes”—*i.e.*, in the ordinary course of business. Plaintiff alleges that each Hospital “use[d] tracking technologies to optimize its website or its marketing for a website”⁹³—indisputably legitimate business purposes.⁹⁴ Moreover, *every* major hospital or health system in Massachusetts has now been sued, facing very similar allegations. Especially under the flexible approach this Court and the Appeals Court have consistently taken to the exception, the Hospitals’ alleged AdTech activities certainly occurred in the

⁹¹ Moreover, software running on computer/tablet/smartphone hardware—the very thing that we use to send and receive emails and text messages and increasingly voice calls—fairly falls within a functional *2020s* definition of “telephone or telegraph equipment.”

⁹² See 49 Mass. App. Ct. at 316.

⁹³ R:A:I:53 (¶ 107); R:A:IV:47 (¶ 97).

⁹⁴ See, e.g., O’Sullivan, 426 Mass. at 265 (secret recordings of calls NYNEX personnel made specifically for marketing purposes fell within the ordinary course of business).

ordinary course of business. Therefore, they could not have violated the Wiretap Act as a matter of law.

The General Court struck a careful balance in 1968—banning surreptitious eavesdropping on interpersonal communications while exempting ordinary course of business activities by legitimate organizations, using standard equipment. Plaintiff wants the benefit of the ban (and the resulting windfall damages) without the counterbalancing hindrance of the exception. That is exactly the type of absurd result, and destruction of the intended legislative balance, that courts consistently reject. This Court should do so again here.

[intentionally blank for formatting reasons on following pages]

VI. Plaintiff Also Lacks Standing.

Plaintiff bears the burden to establish that she has standing to pursue her claims.⁹⁵ At this stage, she must at least plausibly allege that she “has sustained or is immediately in danger of sustaining some direct injury ... that is real and immediate, not conjectural or hypothetical.”⁹⁶ She has not done so, and her failure to carry that burden requires dismissal.⁹⁷

As this Court has explained, “[s]imply alleging injury alone is not sufficient and ‘[i]njuries that are speculative, remote, and indirect’ do not confer proper standing.”⁹⁸ Plaintiff’s complaints do not even reach that insufficient threshold. She claims only a bare statutory violation and alleges nothing about any purported impact on her. The closest she comes is to generally allege that companies such as Google and Meta “can and do identify users on the website and associate their identities to the website users’ communications with the website ... [and] then use the

⁹⁵ See Pugsley v. Police Dep’t of Boston, 472 Mass. 367, 373 (2015).

⁹⁶ See id. at 371 (quoting Los Angeles v. Lyons, 461 U.S. 95, 101-102 (1983)); accord, e.g., HSBC Bank USA, N.A. v. Matt, 464 Mass. 193, 200 (2013); Sullivan v. Chief Justice, 448 Mass. 15, 21 (2006); Enos v. Secretary of Env’t. Affairs, 432 Mass. 132, 135 (2000).

⁹⁷ See, e.g., Matter of Chapman, 482 Mass. 1012, 1015 (2019) (“Standing is not a mere legal technicality. ... if parties do not have standing, a court has no jurisdiction to adjudicate their claims.”); Ginther v. Comm’r of Ins., 427 Mass. 319, 322 (1998) (“We treat standing as an issue of subject matter jurisdiction ... The question of standing is one of critical significance.”) (cleaned up).

⁹⁸ Pugsley, 472 Mass. at 371.

communications to serve personalized advertising to those individuals”⁹⁹—an allegation devoid of (1) anything resembling an injury, and (2) any reference to Plaintiff.

Plaintiff argues the text of § 99(Q) (“[a]ny aggrieved person ... shall have a civil cause of action ... and shall be entitled to recover...”) automatically grants her standing.¹⁰⁰ The Superior Court agreed, ruling that “a properly alleged violation of the [Wiretap Act], alone, constitutes injury sufficient to confer standing.”¹⁰¹ This Court has repeatedly cautioned, however, that “not every party who can claim an injury as a result of violations of a statute or regulation has standing to bring an action thereunder ... [t]his is true even when a literal reading of the statute, without regard to the Legislature’s purpose in enacting it, would appear to provide a broader grant of standing.”¹⁰²

Either the Superior Court erred in ruling that the Act automatically grants standing to all “aggrieved persons,” or the Act’s definition of “aggrieved persons”

⁹⁹ R:A:I:13-14 & R:A:IV:14-15 (¶ 22).

¹⁰⁰ R:A:VII:69-70,81-82 (Opinion and Order at 5-6).

¹⁰¹ R:A:VII:69,81 (Opinion & Order at 5), 103 (BMC Decision at 5).

¹⁰² Beard Motors, Inc. v. Toyota Motor Distribs., Inc., 395 Mass. 428, 431 (1985) (emphasis added); accord, e.g., Ginther, 427 Mass. at 323 (plaintiff must show **both** direct, non-speculative injury **and** that injury fell within statute’s “area of concern”).

was never meant to be stretched so far, or both.¹⁰³ Once again, the stark contrast with the contemporaneous Chapter 93A, discussed above in Section II (pages 27-35), is telling. To pursue a Chapter 93A claim, a plaintiff must show that she “has been injured” by an unfair or deceptive commercial practice.¹⁰⁴ This Court originally ruled that establishing a bare statutory violation was enough,¹⁰⁵ but later (and repeatedly) clarified that plaintiffs must additionally establish a resulting injury.¹⁰⁶

¹⁰³ It is not entirely clear that the General Court has the power to create standing by statute in the absence of concrete, redressable injury. Compare, e.g., TransUnion v. Ramirez, 594 U.S. 413, 426 (2021) (Article III of U.S. Constitution prevents Congress from doing so); with, e.g., Kenn v. Eascare, LLC, No. 22-P-1017, 2024 WL 72736, at *5-8 (Mass. App. Ct. Jan. 8, 2024) (holding that Massachusetts courts are not so limited, but not addressing similar Massachusetts constitutional language in, e.g., part 1, art. XV and part 2, c. 1, § 1, art. III). Even assuming such power exists, there is no reason to believe the General Court actually exercised it in a manner encompassing Plaintiff’s claims. See, e.g., Pishev v. Somerville, 95 Mass. App. Ct. 678, 683 (2019) (“Unless the Legislature has *clearly indicated* that it intends a broader grant of standing, the Supreme Judicial Court has “generally looked to *whether the party claiming to have standing has alleged an injury* ‘within the area of concern of the statute or regulatory scheme under which the injurious action has occurred.’”) (quoting Beard Motors, 395 Mass. at 431) (emphases added).

¹⁰⁴ See G.L. c. 93A, § 9(1).

¹⁰⁵ See Leardi v. Brown, 394 Mass. 151, 160-63 (1985) (“[W]e conclude that, in amending G. L. c. 93A, Section 9, the Legislature exercised its prerogative to create a legal right, the invasion of which, without more, constitutes an injury.”).

¹⁰⁶ See, e.g., Tyler v. Michaels Stores, Inc., 464 Mass. 492, 503 (2013) (“the fact that there is [a c. 93A, § 2] violation does *not* necessarily mean the consumer has suffered an injury or a loss entitling her to at least nominal damages and attorney's fees; instead, the violation of the legal right ... must cause the consumer some kind of *separate, identifiable harm* arising from the violation itself. To the extent ... Leardi can be read ... [otherwise] ... we do not follow the Leardi decision.”) (emphasis added) (citing Rhodes v. AIG Dom. Claims, Inc., 461 Mass. 486, 496

While the Wiretap Act does not include the same “has been injured” language that c. 93A, § 9 features, there is no reason to believe the General Court in the late 1960s intended both: (a) to limit actions alleging unfair and deceptive trade practices only to those plaintiffs who could show actual resulting injury, and (b) to allow *uninjured* plaintiffs to sue for (much larger) liquidated damages under the Wiretap Act. The only plausible explanation, as discussed above, is that the General Court viewed the Wiretap Act’s reach as far more limited than that of Chapter 93A—applying only to unambiguously wrongful acts that inherently would cause compensable injury—*i.e.*, actual, surreptitious eavesdropping on other people’s interpersonal conversations—and not to ordinary practices utilized by thousands of legitimate businesses, non-profit organizations, and government entities.

In short, to the extent the General Court meant to grant standing to all “aggrieved persons” under § 99(Q), it clearly intended that group to be a narrowly-defined, clearly-injured one—not an expansive one. There is no plausible basis on which to think the General Court intended *both* that § 99(Q) could be used like Chapter 93A to police widespread business practices *and* that, *unlike* Chapter 93A, § 99(Q) would provide automatic statutory damages (indeed, 40x the amount)

n.16 (2012); Casavant v. Norwegian Cruise Line Ltd., 460 Mass. 500, 504-505 (2011); Iannacchino v. Ford Motor Co., 451 Mass. 623, 632-633 (2008); Hershenow v. Enterprise Rent-A-Car Co. of Boston, 445 Mass. 790, 801-02 (2006)).

without any showing of actual harm or injury. And yet that is the core assumption on which Plaintiff's claims, and assertions of standing, rely.¹⁰⁷

¹⁰⁷ Plaintiff cites language from this Court's 1989 Pine decision about the "ephemeral quality" of the interests protected by the Wiretap Act leading the General Court to "grant statutory minimum damages without any proof of harm." See 404 Mass. at 418. That language was written in the context of a clear Wiretap Act violation: a landlord's spouse surreptitiously attending and audio recording a meeting between tenants and their lawyers. See id. Plaintiff's allegations here are markedly different. Moreover, the quoted language is *dicta*—having admitted a Wiretap Act violation, the defendants did not contest the plaintiffs' standing or their recovery of actual damages—and, thus, not controlling. See n.78, above. Pine also drew on Leardi's interpretation of Chapter 93A, which this Court subsequently rejected in, *e.g.*, Tyler. See nn. 105 and 106, above. Therefore, Pine is neither controlling nor particularly persuasive on this issue.

CONCLUSION

For all of these reasons, the Hospitals respectfully request that this Court reverse the Superior Court's denials of their motions to dismiss and direct the Superior Court to grant both motions, with prejudice.

Dated: February 7, 2024

Respectfully submitted,

BETH ISRAEL DEACONESS MEDICAL
CENTER, INC. and NEW ENGLAND
BAPTIST HOSPITAL, Defendants-
Appellants

By their attorneys,

/s/ David Quinn Gacioch

David Quinn Gacioch, BBO No. 660784

Annabel Rodriguez, BBO No. 696001

MCDERMOTT WILL & EMERY LLP

200 Clarendon Street, Floor 58

Boston, MA 02116

(617) 535-4000

dgacioch@mwe.com

anrodriguez@mwe.com

ADDENDUM

TABLE OF CONTENTS

Memorandum of Decision and Order and Report to the Appeals Court in Vita v. Beth Israel Deaconess Medical Center, Inc., 2384cv00480-BLS160

Memorandum of Decision and Order and Report to the Appeals Court in Vita v. New England Baptist Hospital, 2384cv00857-BLS172

G.L. c. 272, § 99.84

NOTIFY

17

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT
CIVIL ACTION
No. 2384CV00480-BLS1

KATHLEEN VITA¹

vs.

BETH ISRAEL DEACONESS MEDICAL CENTER, INC.

**MEMORANDUM OF DECISION AND ORDER ON
DEFENDANT'S MOTION TO DISMISS
AND REPORT TO THE APPEALS COURT**

Plaintiff Kathleen Vita ("Plaintiff") commenced this putative class action against defendant Beth Israel Deaconess Medical Center ("BIDMC"), alleging that it used internet tracking tools on its website that illegally redirected website users' personal information, and the contents of users' communications with BIDMC's website, to third parties Google and Meta. On the basis of these allegations, the Complaint asserts a single claim for violation of the Massachusetts Wiretap Statute, G.L. c. 272, § 99. Presently before the court is BIDMC's motion to dismiss. After a hearing on September 19, 2023, and consideration of the parties' submissions, the motion is **DENIED**, and, consistent with the parties' request, the matter is **REPORTED** to the Appeals Court.

BACKGROUND

The Complaint and relevant documents attached to the motion to dismiss set forth the following facts.² BIDMC operates a hospital in Boston that offers inpatient and outpatient care

¹ For herself and the class.

² BIDMC's complete website Privacy Policy, which Plaintiff relies on in framing her Complaint, was attached to the motion to dismiss. *Marram v. Kobrick Offshore Fund, Ltd.*, 442 Mass. 43, 45 n.4 (2004).

to residents in the greater Boston area. Plaintiff is an individual residing in Revere, Massachusetts.

BIDMC maintains and controls a website for its hospital. The website allows users to obtain information about the services BIDMC provides, including information about doctors, services, and treatments provided for particular medical conditions. Website users also can book appointments, access and pay bills, and access private medical information through the website's patient portal. The website contains search bars that aid users in finding specific information on the site, and forms that users may submit to BIDMC, such as the "Request an Appointment" form.

As relevant here, BIDMC's website privacy policy ("Privacy Policy") states:

Beth Israel Deaconess Medical Center (BIDMC) is committed to protecting your privacy. The BIDMC website allows you to visit most areas without identifying yourself or providing personal information. For those areas where you elect to provide identifiable information, we assure you that we make every effort to protect your privacy. . . .

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. Except for authorized law enforcement investigations or other facially valid legal processes, we will not share any information we receive with outside parties. . . .

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, and completion status of the request. These logs may be kept for an indefinite amount of time, used at any time and in any way necessary to prevent security breaches and to ensure the integrity of the data on our servers.

(Formatting altered). Since 2021, BIDMC's website also has included a pop-up notice that references the use of "cookies and other tools to enhance your experience on the website," with a link to the Privacy Policy "for more information about these cookies and the data collected."

Notwithstanding this Privacy Policy, BIDMC has implemented multiple software-based internet tracking technologies on its website that contemporaneously record and transmit data about users' interactions with BIDMC's website to multiple unidentified third parties. The software is unrelated to the website's functionality and is invisible to users. Two such tracking technologies are Meta Pixel, which transmits data to Meta (the parent company of Facebook), and Google Analytics, which transmits data to Google.

Meta Pixel and Google Analytics operate through the automatic execution of pieces of JavaScript code, embedded in the BIDMC website, which cause a website user's internet browser to record and send information to those third parties when a user visits and interacts with the site. The transmitted information can include: the website address (URL); the title of webpages visited; information about the content of the website; search terms or any other information inputted into a form; selections on drop-down menus and the contents thereof; scrolls down a webpage; and button clicks. A website user's internet protocol ("IP") address and web browser configurations are also revealed, which permits Google and Meta to associate the data it receives from the website visit to the identity of a particular individual known to them. The content of the user's communications with BIDMC's website is added to Google's and Meta's collection of information already known about the individual, which can be used to target advertising to that individual. Google, Meta, and BIDMC may also use the information collected for other commercial purposes. After a media exposé about the use of Meta Pixel on hospital

websites, BIDMC removed it from its website in September 2022. As of the date the Complaint was filed, Google Analytics software remained on the BIDMC website.

In addition to Meta Pixel and Google Analytics, BIDMC also employs other software-based internet tracking technologies that work in a similar fashion. Those include Doubleclick, Siteimprove Analytics, and Marchex.io.

Plaintiff's husband is a BIDMC patient. Plaintiff regularly uses the BIDMC website to obtain information about BIDMC doctors (including their credentials and backgrounds); search for information on particular symptoms, conditions, and medical procedures, both for herself and her husband; and obtain and review her husband's medical records through the BIDMC website patient portal.

STANDARD OF REVIEW

Rule 12(b)(6) allows for dismissal of a complaint when the factual allegations contained within it do not suggest a plausible entitlement to relief. *Iannacchino v. Ford Motor Co.*, 451 Mass. 623, 635-636 (2008); *Fraelick v. PerketPR, Inc.*, 83 Mass. App. Ct. 698, 699-700 (2013). In ruling on the motions, the court accepts the factual allegations as true and draws all reasonable inferences in the non-moving party's favor. *Fraelick*, 83 Mass. App. Ct. at 699-700.

DISCUSSION

BIDMC argues that Plaintiff's claims must be dismissed due to lack of standing and failure to meet the requirements of the Massachusetts Wiretap Statute. As discussed below, however, under this court's reading of the relevant caselaw and the plain language of the statute, the Complaint states a claim sufficient to survive dismissal under Rule 12(b)(6). Nevertheless, because of the novelty of the issue raised, which also has arisen in several analogous cases

before this court, and for the further reasons discussed below, a report to the Appeals Court is appropriate.³

1. Standing⁴

This court recently addressed standing in an analogous wiretap cases — *Doe v. Boston Medical Center*, 2384CV00326-BLS1, slip op. at 4-5 (Mass. Super. Ct. Sept. 15, 2023) (“*Boston Medical Center*”). There, the court denied the defendant’s motion to dismiss on standing grounds, concluding that “a properly alleged violation of the [Massachusetts Wiretap Statute], alone, constitute[s] injury sufficient to confer standing.” *Id.* (citing *Pine v. Rust*, 404 Mass. 411, 418 (1989); *In re Lubanski*, 186 B.R. 160, 166-67 (Bankr. D. Mass. 1995)). For the same reasons enunciated in that decision, Plaintiff has standing to sue here, as well.

2. Massachusetts Wiretap Statute

General Laws c. 272, § 99(Q) provides a cause of action for “any aggrieved person whose oral or wire communications were intercepted, disclosed or used . . . or whose personal or property interests or privacy were violated by means of an interception,” except as permitted or authorized by the Wiretap Statute. “Interception” is defined to mean “to secretly hear, secretly record, or aid 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).

BIDMC argues that the action should be dismissed because, according to it: 1) the statute applies only to “conversations,” not internet tracking; 2) BIDMC’s recording of website user

³ On this same date the court also decides a similar motion to dismiss and reports the correctness of its ruling to the Appeals Court in *Kathleen Vita v. New England Baptist Hospital*, 2384CV00857-BLS1.

⁴ The standard of review for challenging standing in a motion to dismiss under Rule 12(b)(1) is functionally the same as under Rule 12(b)(6). *Abate v. Fremont Inv. & Loan*, 470 Mass. 821, 828 (2015).

activity was not secret; 3) the statutory “ordinary course of business” exception applies; and 4) application of the statute to the facts here would lead to absurd results the Legislature could not have intended. The court addresses each, in turn.

A. Limitation of the statute to human-to-human conversation. In prior analogous cases, this court concluded that the plain language of the statute encompasses the electronic activity alleged here. *See Boston Medical Center*, 2384CV00326-BLS1, slip op. at 6-7; *Doe v. Boston Children’s Hospital*, 2384CV00411-BLS1, slip op. at 4-6 (Mass. Super. Ct. Sept. 15, 2023) (“*Boston Children’s*”). Accordingly, for the same reasons already articulated in those cases, the argument fails here, as well.

B. Secrecy requirement. As noted, an interception under the Massachusetts Wiretap Statute must be “secret.” G.L. c. 272, § 99(B)(4). A “secret” recording is one that is “concealed,” and “kept hidden or unexplained.” *Curtatone v. Barstool Sports, Inc.*, 487 Mass. 655, 658 (2021) (dictionary citations omitted). An interception is not secret for purposes of the Massachusetts Wiretap Statute if the individual communicating has “actual [or constructive] knowledge of the recording,” which is proved through “‘clear and unequivocal objective manifestations of knowledge’ in the [users’] statements or conduct.” *Commonwealth v. Morris*, 492 Mass. 498, 515 (2023) (Budd., J., concurring) (quoting *Commonwealth v. Jackson*, 370 Mass. 502, 507 (1976)). *See Commonwealth v. Du*, No. 22-P-870, 2023 WL 652243, at *6 (Mass. App. Ct. Oct. 6, 2023).

BIDMC argues that its Privacy Policy and related website pop-up disclose BIDMC’s collection of data, and its sharing of that data with a third party, such that the internet tracking activity alleged here is not secret. There are two problems with that argument. First, the Privacy Policy is unclear about the exact nature of the website data BIDMC shares. The Privacy Policy

informs users that BIDMC collects certain user data that is kept anonymous and which “is not shared with other organizations,” but then notes the existence of an external “Third Party Service Provider” that also collects data, but defines that collected data in a different way. The Privacy Policy language is technical and obscures whether the BIDMC data and the Third Party Service Provider data are related or overlap in some ways, and thus whether some of the purportedly private, unshared, “anonymous” data BIDMC collects is nevertheless shared with the Third Party Service Provider.⁵ Second, the Privacy Policy discloses the existence of only a *single* “Third Party Service Provider,” while the Complaint alleges that the data BIDMC collects is contemporaneously shared with *multiple* external organizations (Google, Meta, and others). The existence of these additional third-party “eavesdroppers” are thus kept hidden from BIDMC’s website users.

In sum, the Privacy Policy and website pop-up, while disclosing some amount of data sharing, do not establish users’ actual or constructive knowledge of the totality of the internet tracking alleged here.⁶ Accordingly, on the facts as pleaded and taken as true, the Complaint sufficiently alleges a secret interception, i.e. that BIDMC “aid[ed] another to secretly hear or secretly record the contents of any wire or oral communication.” G.L. c. 272, § 99(B)(4).⁷

C. “*Ordinary course of business*” exception. The Massachusetts Wiretap Statute excepts from the definition of “intercepting device”:

⁵ Indeed, as a lay reader of the Privacy Policy, the court is unable to determine whether BIDMC’s collected data about “how many people visit the site, the pages they visit, where they come from, how long they stay, etc.” includes some of the same information as it and the Third Party Service Provider’s collection of “default information customarily logged by worldwide web server software.”

⁶ That a website user can reveal the internet tracking software code by employing “Developer Mode” also does not establish actual or constructive knowledge of the software code at issue.

⁷ Because this case alleges third-party eavesdropping on website communications by undisclosed, contemporaneous third-parties, this case differs from *Curtatone v. Barstool Sports, Inc.*, 487 Mass. 655 (2023), which involved a consented-to recorded conversation between two people only. *See id.* at 657, 660.

any telephone or telegraph instrument, equipment, facility, or a component thereof, (a) furnished to a subscriber or user by a communications common carrier in the ordinary course of its business under its tariff and being used by the subscriber or user in the ordinary course of its business . . .

G.L. c. 272, § 99(B)(3). Thus, for the exception to apply, the intercepting device at issue must consist of or include “telephone or telegraph” equipment, instruments, etc. *Id.*

Setting aside whether internet tracking occurs in the ordinary course of BIDMC’s business, the electronic software-based internet tracking technology at issue here plainly is not telephone or telegraph equipment. For that reason, in the absence of an appellate decision extending the exception beyond the realm of telephones and telegraphs, under the plain language of the statute, the court declines to apply the exception here. *See Alves v. BJ’s Wholesale Club, Inc.*, 2284CV02509-BLS1, slip op. at 10 (Super. Ct. June 21, 2023) (“*Alves*”) (declining to extend exception to software-based session replay code technology).

D. Legislative Intent. Finally, BIDMC argues that interpreting the Massachusetts Wiretap Statute to encompass the ubiquitous internet tracking that practically all businesses presently employ would lead to absurd results the Legislature could not have intended when it enacted the statute in 1968. Reading the criminal caselaw that BIDMC cites for this proposition does not compel the denial it seeks, however.

Commonwealth v. Morris, 492 Mass. 498 (2023), and *Commonwealth v. Rainey*, 491 Mass. 632 (2023), upon which BIDMC relies, each involve statements made to police wherein the speakers necessarily understood that their statements were being memorialized for future use or presentation in court, despite the lack of explicit disclosure about electronic recording. *Morris*, 492 Mass. at 503-04; *Rainey*, 491 Mass. at 635, 640-41. In that narrow context, the

court determined that literal application of the Massachusetts Wiretap Statute would result in absurd and unintended consequences, at odds with the Legislature's intent in enacting the statute. *See Morris*, 492 Mass. at 506 ("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"); *Rainey*, 491 Mass. at 643 (same as to victim's voluntarily-provided statement to police).

Here, unlike the criminal defendant and victim in *Morris* and *Rainey*, Plaintiff and BIDMC's other website users 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. Rather, the entire gist of the Complaint is that Plaintiff interacted with the BIDMC website with no concept that the data she inputted would be simultaneously and automatically intercepted and externally shared with multiple external parties. These facts alone distinguish this case from *Morris* and *Rainey*.

In further contrast to those cases, the statute's preamble arguably supports the right to freedom from private electronic surveillance at issue here. Its broad language provides:

The general court . . . finds that the uncontrolled development and unrestricted use of modern electronic surveillance devices pose grave dangers to the privacy of all citizens of the commonwealth. Therefore, the secret use of such devices by private individuals must be prohibited.

G.L. c. 272, § 99. In fact, a broad interpretation of the statute's language is endorsed in *Commonwealth v. Moody*, 466 Mass. 196 (2013), a Supreme Judicial Court decision that

extended the Massachusetts Wiretap Statute’s application to electronic text messages. *See id.* at 209 (“[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”).⁸

For the reasons explained above, and absent an appellate decision interpreting the Massachusetts Wiretap Statute in the narrow way that BIDMC suggests, this court concludes that the facts as alleged in the Complaint state a claim for a violation of the statute.

3. Report to Appeals Court

Under Mass. R. Civ. P. 64, a Superior Court judge may report an interlocutory decision “where he or she concludes that the finding or order ‘so affects the merits of the controversy that the matter ought to be determined by the [A]ppeals [C]ourt before any further proceedings in the trial court.’” *Patel v. Martin*, 481 Mass. 29, 32 (2018) (quoting Mass. R. Civ. P. 64(a)). The Supreme Judicial Court has cautioned that “[i]nterlocutory matters should be reported only where it appears that they present serious questions likely to be material in the ultimate decision, and that subsequent proceedings in the trial court will be substantially facilitated by so doing.” *Globe Newspaper Co. v. Massachusetts Bay Transp. Auth. Ret. Bd.*, 412 Mass. 770, 772 (1992) (quoting *John Gilbert Jr. Co. v. C.M. Fauci Co.*, 309 Mass. 271, 273 (1941)). Such is the case here. The parties here also have requested that the court report the matter to the Appeals Court.

Whether the Massachusetts Wiretap Statute applies to the internet tracking alleged here is a novel question unresolved at the appellate level in Massachusetts, and is the central and

⁸ The most recent published case interpreting the Massachusetts Wiretap Statute is consistent with this view. *See Commonwealth v. Du*, No. 22-P-870, 2023 WL 6522435, at *6-*7 (Mass. App. Ct. Oct. 6, 2023) (court interpreted statute to prohibit surreptitious audio-visual video recording of drug transaction made by police using cell phone application).

dispositive issue in this case. Although the Massachusetts Wiretap Statute is broadly drafted, and states the Legislature's explicit intention to protect citizens from the grave danger of electronic surveillance by private individuals poses, it was enacted in 1968 — long before the internet, let alone internet tracking, became available. The Legislature did not, therefore, contemplate internet tracking as a form of secretly intercepting communications. BIDMC argues that internet tracking is practically ubiquitous across all businesses and organizations with websites, and that BIDMC's use of such tracking is a legitimate, ordinary part of its business. Had the Legislature been aware of internet tracking and its possible business uses in 1968, it might have written the statute to allow the type of tracking alleged in this case.

The novel question here has arisen in several other cases. As noted, this court already has denied motions to dismiss in two other internet-tracking wiretap cases. *See Boston Medical Center*, 2384CV00326-BLS1; *Boston Children's*, 2384CV00411-BLS1. Other Superior Court judges have issued similar decisions. *See Alves*, 2284CV02509-BLS1; *Doe v. Partners Healthcare System, Inc.*, 1984CV01651-BLS1, endorsement denying motion to dismiss (Super. Ct. Dec. 7, 2020). There are many other analogous cases presently pending in the Superior Court, including in this session.⁹ If, as BIDMC argues, the Massachusetts Wiretap Statute does not apply to business-related internet tracking, significant judicial and party resources will be saved by the quick resolution of these cases before discovery and other stages of litigation.

⁹ Other analogous cases pending in BLS1 include: *Progin, Janice v. UMass Memorial Health Care, Inc.*, 2284CV2889; *John Doe v. Boston Medical Center Corp.*, 2384CV326; *Jane Doe v. The Children's Hospital Corp.*, 2384CV411; *Kathleen Vita v. New England Baptist Hospital*, 2384CV00857; *Karen McManus v. Tufts Medical Center, Inc.*, 2384CV930; *Elizabeth Nova v. Boston Medical Center Corporation*, 2384CV1086; *Jane Doe v. Cape Cod Healthcare, Inc.*, 2384CV1236; *Jane Doe v. Baystate Health Systems*, 2384CV1949; *John Doe v. UMass Memorial Health Care Inc.*, 2384CV2448; *Lisa Colleton v. UMass Memorial Health Care Inc.*, 2384CV2450

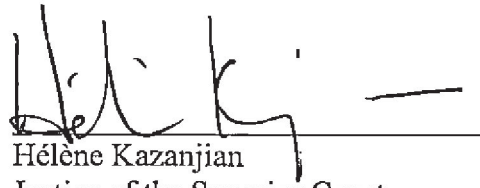
For all of these reasons, this matter should be determined by the Appeals Court before any proceedings continue in this court.

ORDER

For the foregoing reasons, it is hereby **ORDERED** that:

1. BIDMC's motion to dismiss is **DENIED**; and
2. The Court **REPORTS** the correctness of its ruling to the Appeals Court.

Dated: October 31, 2023


Hélène Kazanjian
Justice of the Superior Court

NOTIFY

16

COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss.

SUPERIOR COURT
CIVIL ACTION
No. 2384CV00857-BLS1

KATHLEEN VITA¹

11/1/23
notice sent
BH (2)

vs.

NEW ENGLAND BAPTIST HOSPITAL

MEMORANDUM OF DECISION AND ORDER ON
DEFENDANT'S MOTION TO DISMISS
AND REPORT TO THE APPEALS COURT

Plaintiff Kathleen Vita ("Plaintiff") commenced this putative class action against defendant New England Baptist Hospital ("NEBH"), alleging that it used internet tracking tools on its website that illegally redirected website users' personal information, and the contents of users' communications with NEBH's website, to third parties Google and Meta. On the basis of these allegations, the Complaint asserts a single claim for violation of the Massachusetts Wiretap Statute, G.L. c. 272, § 99. Presently before the court is NEBH's motion to dismiss. After a hearing on September 19, 2023, and consideration of the parties' submissions, the motion is **DENIED**, and, consistent with the parties' request, the matter is **REPORTED** to the Appeals Court.

BACKGROUND

The Complaint and relevant documents attached to the motion to dismiss set forth the following facts.² NEBH operates a hospital with a main campus in Boston, and several other

¹ For herself and the class.

² NEBH's complete website Privacy Policy, which Plaintiff relies on in framing her Complaint, was attached to the motion to dismiss. *Marram v. Kobrick Offshore Fund, Ltd.*, 442 Mass. 43, 45 n.4 (2004).

locations in the Boston area, focusing on orthopedic care and complex orthopedic procedures. Plaintiff is an individual residing in Revere, Massachusetts.

NEBH maintains and controls a website for its hospital. The website allows users to obtain information about the services NEBH provides, including information about doctors, services, and treatments provided for particular medical conditions. Website users also can access and pay bills, and access private medical information through the website's patient portal. The website contains search bars that aid users in finding specific information on the site, and forms that users may submit to NEBH, such as the "Find a Doctor" form.

As relevant here, NEBH's website privacy policy ("Privacy Policy") states:

New England Baptist Hospital (NEBH) is committed to protecting your privacy. The NEBH website allows you to visit most areas without identifying yourself or providing personal information. For those areas where you elect to provide identifiable information, we assure you that we make every effort to protect your privacy. . . .

New England Baptist Hospital 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. Except for authorized law enforcement investigations or other facially valid legal processes, we will not share any information we receive with outside parties. . . .

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, and completion status of the request. These logs may be kept for an indefinite amount of time, used at any time and in any way necessary to prevent security breaches and to ensure the integrity of the data on our servers.

(Formatting altered). Since 2021, NEBH's website also has included a pop-up notice that references the use of "cookies and other tools to enhance your experience on the

website,” with a link to the Privacy Policy “for more information about these cookies and the data collected.”

Notwithstanding this Privacy Policy, NEBH has implemented multiple software-based internet tracking technologies on its website that contemporaneously record and transmit data about users’ interactions with NEBH’s website to multiple unidentified third parties. The software is unrelated to the website’s functionality and is invisible to users. Two such tracking technologies are Meta Pixel, which transmits data to Meta (the parent company of Facebook), and Google Analytics, which transmits data to Google.

Meta Pixel and Google Analytics operate through the automatic execution of pieces of JavaScript code, embedded in the NEBH website, which cause a website user’s internet browser to record and send information to those third parties when a user visits and interacts with the site. The transmitted information can include: the website address (URL); the title of webpages visited; information about the content of the website; search terms or any other information inputted into a form; selections on drop-down menus and the contents thereof; scrolls down a webpage; and button clicks. A website user’s internet protocol (“IP”) address and web browser configurations are also revealed, which permits Google and Meta to associate the data it receives from the website visit to the identity of a particular individual known to them. The content of the user’s communications with NEBH’s website is added to Google’s and Meta’s collection of information already known about the individual, which can be used to target advertising to that individual. Google, Meta, and NEBH may also use the information collected for other commercial purposes. After a media exposé about the use of Meta Pixel on hospital websites in June 2022, NEBH removed it from its website at some unidentified point in time. As of the date the Complaint was filed, Google Analytics software remained on the NEBH website.

Plaintiff is a NEBH patient. Plaintiff regularly uses the NEBH website to obtain information about NEBH doctors (including their credentials and backgrounds) and to search for information on particular medical procedures.

STANDARD OF REVIEW

Rule 12(b)(6) allows for dismissal of a complaint when the factual allegations contained within it do not suggest a plausible entitlement to relief. *Iannacchino v. Ford Motor Co.*, 451 Mass. 623, 635-636 (2008); *Fraelick v. Perket PR, Inc.*, 83 Mass. App. Ct. 698, 699-700 (2013). In ruling on the motions, the court accepts the factual allegations as true and draws all reasonable inferences in the non-moving party's favor. *Fraelick*, 83 Mass. App. Ct. at 699-700.

DISCUSSION

NEBH argues that Plaintiff's claims must be dismissed due to lack of standing and failure to meet the requirements of the Massachusetts Wiretap Statute. As discussed below, however, under this court's reading of the relevant caselaw and the plain language of the statute, the Complaint states a claim sufficient to survive dismissal under Rule 12(b)(6). Nevertheless, because of the novelty of the issue raised, which also has arisen in several analogous cases before this court, and for the further reasons discussed below, a report to the Appeals Court is appropriate.³

³ On this same date the court also decides a similar motion to dismiss and reports the correctness of its ruling to the Appeals Court in *Kathleen Vita v. Beth Israel Deaconess Medical Center, Inc.*, 2384CV00480-BLS1.

1. Standing⁴

This court recently addressed standing in an analogous wiretap case — *Doe v. Boston Medical Center*, 2384CV00326-BLS1, slip op. at 4-5 (Mass. Super. Ct. Sept. 15, 2023) (“*Boston Medical Center*”). There, the court denied the defendant’s motion to dismiss on standing grounds, concluding that “a properly alleged violation of the [Massachusetts Wiretap Statute], alone, constitute[s] injury sufficient to confer standing.” *Id.* (citing *Pine v. Rust*, 404 Mass. 411, 418 (1989); *In re Lubanski*, 186 B.R. 160, 166-67 (Bankr. D. Mass. 1995)). For the same reasons enunciated in that decision, Plaintiff has standing to sue here, as well.

2. Massachusetts Wiretap Statute

General Laws c. 272, § 99(Q) provides a cause of action for “any aggrieved person whose oral or wire communications were intercepted, disclosed or used . . . or whose personal or property interests or privacy were violated by means of an interception,” except as permitted or authorized by the Wiretap Statute. “Interception” is defined to mean “to secretly hear, secretly record, or aid 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).

NEBH argues that the action should be dismissed because, according to it: 1) the statute applies only to “conversations,” not internet tracking; 2) NEBH’s recording of website user activity was not secret; 3) the statutory “ordinary course of business” exception applies; and 4) application of the statute to the facts here would lead to absurd results the Legislature could not have intended. The court addresses each, in turn.

⁴ The standard of review for challenging standing in a motion to dismiss under Rule 12(b)(1) is functionally the same as under Rule 12(b)(6). *Abate v. Fremont Inv. & Loan*, 470 Mass. 821, 828 (2015).

A. Limitation of the statute to human-to-human conversation. In prior analogous cases, this court concluded that the plain language of the statute encompasses the electronic activity alleged here. See *Boston Medical Center*, 2384CV00326-BLS1, slip op. at 6-7; *Doe v. Boston Children's Hospital*, 2384CV00411-BLS1, slip op. at 4-6 (Mass. Super. Ct. Sept. 15, 2023) ("*Boston Children's*"). Accordingly, for the same reasons articulated in those cases, the argument fails here, as well.

B. Secrecy requirement. As noted, an interception under the Massachusetts Wiretap Statute must be "secret." G.L. c. 272, § 99(B)(4). A "secret" recording is one that is "concealed," and "kept hidden or unexplained." *Curtatone v. Barstool Sports, Inc.*, 487 Mass. 655, 658 (2021) (dictionary citations omitted). An interception is not secret for purposes of the Massachusetts Wiretap Statute if the individual communicating has "actual [or constructive] knowledge of the recording," which is proved through "'clear and unequivocal objective manifestations of knowledge' in the [users'] statements or conduct." *Commonwealth v. Morris*, 492 Mass. 498, 515 (2023) (Budd., J., concurring) (quoting *Commonwealth v. Jackson*, 370 Mass. 502, 507 (1976)). See *Commonwealth v. Du*, No. 22-P-870, 2023 WL 652243, at *6 (Mass. App. Ct. Oct. 6, 2023).

NEBH argues that its Privacy Policy and related website pop-up disclose NEBH's collection of data, and its sharing of that data with a third party, such that the internet tracking activity alleged here is not secret. There are two problems with that argument. First, the Privacy Policy is unclear about the exact nature of the website data NEBH shares. The Privacy Policy informs users that NEBH collects certain user data that is kept anonymous and which "is not shared with other organizations," but then notes the existence of an external "Third Party Service Provider" that also collects data, but defines that collected data in a different way. The Privacy

Policy language is technical and obscures whether the NEBH data and the Third Party Service Provider data are related or overlap in some ways, and thus whether some of the purportedly private, unshared, “anonymous” data NEBH collects is nevertheless also shared with the Third Party Service Provider.⁵ Second, the Privacy Policy discloses the existence of only a *single* “Third Party Service Provider,” while the Complaint alleges that the data NEBH collects is contemporaneously shared with *multiple* external organizations (Google, Meta, and others). The existence of these additional third-party “eavesdroppers” are thus kept hidden from NEBH’s website users.

In sum, the Privacy Policy and website pop-up, while disclosing some amount of data sharing, do not establish users’ actual or constructive knowledge of the totality of the internet tracking alleged here.⁶ Accordingly, on the facts as pleaded and taken as true, the Complaint sufficiently alleges a secret interception, i.e. that NEBH “aid[ed] another to secretly hear or secretly record the contents of any wire or oral communication.” G.L. c. 272, § 99(B)(4).⁷

C. “Ordinary course of business” exception. The Massachusetts Wiretap Statute exempts from the definition of “intercepting device”:

any telephone or telegraph instrument, equipment, facility, or a component thereof, (a) furnished to a subscriber or user by a communications common carrier in the ordinary course of its business under its tariff and being used by the subscriber or user in the ordinary course of its business . . .

⁵ Indeed, as a lay reader of the Privacy Policy, the court is unable to determine whether NEBH’s collected data about “how many people visit the site, the pages they visit, where they come from, how long they stay, etc.” includes some of the same information as it and the Third Party Service Provider’s collection of “default information customarily logged by worldwide web server software.”

⁶ That a website user can reveal the internet tracking software code by employing “Developer Mode” also does not establish actual or constructive knowledge of the software code at issue.

⁷ Because this case alleges third-party eavesdropping on website communications by undisclosed, contemporaneous third-parties, this case differs from *Curtatone v. Barstool Sports, Inc.*, 487 Mass. 655 (2023), which involved a consented-to recorded conversation between two people only. *See id.* at 657, 660.

G.L. c. 272, § 99(B)(3). Thus, for the exception to apply, the intercepting device at issue must consist of or include “telephone or telegraph” equipment, instruments, etc. *Id.*

Setting aside whether internet tracking occurs in the ordinary course of NEBH’s business, the electronic software-based internet tracking technology at issue here plainly is not telephone or telegraph equipment. For that reason, in the absence of an appellate decision extending the exception beyond telephones and telegraphs, under the plain language of the statute, the court declines to apply the exception here. *See Alves v. BJ’s Wholesale Club, Inc.*, 2284CV02509-BLS1, slip op. at 10 (Super. Ct. June 21, 2023) (“*Alves*”) (declining to extend exception to software-based session replay code technology).

D. Legislative Intent. Finally, NEBH argues that interpreting the Massachusetts Wiretap Statute to encompass the ubiquitous internet tracking that practically all businesses presently employ would lead to absurd results the Legislature could not have intended when it enacted the statute in 1968. Reading the criminal caselaw that NEBH cites for this proposition does not compel the denial it seeks, however.

Commonwealth v. Morris, 492 Mass. 498 (2023), and *Commonwealth v. Rainey*, 491 Mass. 632 (2023), upon which NEBH relies, each involve statements made to police where the speakers necessarily understood that their statements were being memorialized for future use or presentation in court, despite the lack of explicit disclosure about electronic recording. *Morris*, 492 Mass. at 503-04; *Rainey*, 491 Mass. at 635, 640-41. In that narrow context, the court determined that literal application of the Massachusetts Wiretap Statute would result in absurd and unintended consequences, at odds with the Legislature’s intent in enacting the statute. *See Morris*, 492 Mass. at 506 (“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"); *Rainey*, 491 Mass. at 643 (same as to victim's voluntarily-provided statement to police).

Here, unlike the criminal defendant and victim in *Morris* and *Rainey*, Plaintiff and NEBH's other website users 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. Rather, the entire gist of the Complaint is that Plaintiff interacted with the NEBH website with no concept that the data she inputted would be simultaneously and automatically intercepted and externally shared with multiple external parties. These facts alone distinguish this case from *Morris* and *Rainey*.

In further contrast to those cases, the statute's preamble arguably supports the right to freedom from private electronic surveillance at issue here. Its broad language provides:

The general court . . . finds that the uncontrolled development and unrestricted use of modern electronic surveillance devices pose grave dangers to the privacy of all citizens of the commonwealth. Therefore, the secret use of such devices by private individuals must be prohibited.

G.L. c. 272, § 99. In fact, a broad interpretation of the statute's language is endorsed in *Commonwealth v. Moody*, 466 Mass. 196 (2013), a Supreme Judicial Court decision that extended the Massachusetts Wiretap Statute's application to electronic text messages. *See id.* at 209 ("[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”).⁸

For the reasons explained above, and absent an appellate decision interpreting the Massachusetts Wiretap Statute in the narrow way that NEBH suggests, this court concludes that the facts as alleged in the Complaint state a claim for a violation of the statute.

3. Report to Appeals Court

Under Mass. R. Civ. P. 64, a Superior Court judge may report an interlocutory decision “where he or she concludes that the finding or order ‘so affects the merits of the controversy that the matter ought to be determined by the [A]ppeals [C]ourt before any further proceedings in the trial court.’” *Patel v. Martin*, 481 Mass. 29, 32 (2018) (quoting Mass. R. Civ. P. 64(a)). The Supreme Judicial Court has cautioned that “[i]nterlocutory matters should be reported only where it appears that they present serious questions likely to be material in the ultimate decision, and that subsequent proceedings in the trial court will be substantially facilitated by so doing.” *Globe Newspaper Co. v. Massachusetts Bay Transp. Auth. Ret. Bd.*, 412 Mass. 770, 772 (1992) (quoting *John Gilbert Jr. Co. v. C.M. Fauci Co.*, 309 Mass. 271, 273 (1941)). Such is the case here. The parties here also have requested that the court report the matter to the Appeals Court.

Whether the Massachusetts Wiretap Statute applies to the internet tracking alleged here is a novel question unresolved at the appellate level in Massachusetts, and is the central and dispositive issue in this case. Although the Massachusetts Wiretap Statute is broadly drafted, and states the Legislature’s explicit intention to protect citizens from the grave danger of

⁸ The most recent published case interpreting the Massachusetts Wiretap Statute is consistent with this view. See *Commonwealth v. Du*, No. 22-P-870, 2023 WL 6522435, at *6-*7 (Mass. App. Ct. Oct. 6, 2023) (court interpreted statute to prohibit surreptitious audio-visual video recording of drug transaction made by police using cell phone application).

electronic surveillance by private individuals, it was enacted in 1968 — long before the internet, let alone internet tracking, became available. The Legislature did not, therefore, contemplate internet tracking as a form of secretly intercepting communications. NEBH argues that internet tracking is practically ubiquitous across all businesses and organizations with websites, and that NEBH's use of such tracking is a legitimate, ordinary part of its business. Had the Legislature been aware of internet tracking and its possible business uses in 1968, it might have written the statute to allow the type of tracking alleged in this case.

The novel question here has arisen in several other cases. As noted, this court already has denied motions to dismiss in two other internet-tracking wiretap cases. *See Boston Medical Center*, 2384CV00326-BLS1; *Boston Children's*, 2384CV00411-BLS1. Other Superior Court judges have issued similar decisions recently. *See Alves*, 2284CV02509-BLS1; *Doe v. Partners Healthcare System, Inc.*, 1984CV01651-BLS1, endorsement denying motion to dismiss (Super. Ct. Dec. 7, 2020). There are many other analogous cases presently pending in the Superior Court, including in this session.⁹ If, as NEBH argues, the Massachusetts Wiretap Statute does not apply to business-related internet tracking, significant judicial and party resources will be saved by the quick resolution of these cases before discovery and other stages of litigation.

For all of these reasons, this matter should be determined by the Appeals Court before any proceedings continue in this court.

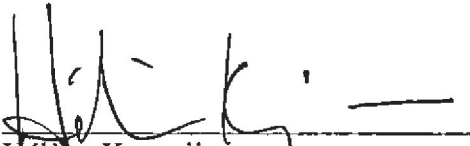
⁹ Other analogous cases pending in BLS1 include: *Progin, Janice v. UMass Memorial Health Care, Inc.*, 2284CV2889; *John Doe v. Boston Medical Center Corp.*, 2384CV326; *Jane Doe v. The Children's Hospital Corp.*, 2384CV411; *Kathleen Vita v. Beth Israel Deaconess Medical Center, Inc.*, 2384CV00480; *Karen McMamus v. Tufts Medical Center, Inc.*, 2384CV930; *Elizabeth Nova v. Boston Medical Center Corporation*, 2384CV1086; *Jane Doe v. Cape Cod Healthcare, Inc.*, 2384CV1236; *Jane Doe v. Baystate Health Systems*, 2384CV1949; *John Doe v. UMass Memorial Health Care Inc.*, 2384CV2448; *Lisa Colleton v. UMass Memorial Health Care Inc.*, 2384CV2450

ORDER

For the foregoing reasons, it is hereby **ORDERED** that:

1. NEBH's motion to dismiss is **DENIED**; and
2. The Court **REPORTS** the correctness of its ruling to the Appeals Court.

Dated: October 31, 2023


Héline Kazanjian
Justice of the Superior Court

Part IV	CRIMES, PUNISHMENTS AND PROCEEDINGS IN CRIMINAL CASES
Title I	CRIMES AND PUNISHMENTS
Chapter 272	CRIMES AGAINST CHASTITY, MORALITY, DECENCY AND GOOD ORDER
Section 99	INTERCEPTION OF WIRE AND ORAL COMMUNICATIONS

Section 99. Interception of wire and oral communications.—

A. Preamble.

The general court finds that organized crime exists within the commonwealth and that the increasing activities of organized crime constitute a grave danger to the public welfare and safety. Organized crime, as it exists in the commonwealth today, consists of a continuing conspiracy among highly organized and disciplined groups to engage in supplying illegal goods and services. In supplying these goods and services organized crime commits unlawful acts and employs brutal and violent tactics. Organized crime is infiltrating legitimate business activities and depriving honest businessmen of the right to make a living. The general court further finds that because organized crime carries on its activities through layers of insulation and behind a wall of secrecy, government has been unsuccessful in curtailing and eliminating it. Normal investigative procedures are not effective in the investigation of

illegal acts committed by organized crime. Therefore, law enforcement officials must be permitted to use modern methods of electronic surveillance, under strict judicial supervision, when investigating these organized criminal activities.

The general court further finds that the uncontrolled development and unrestricted use of modern electronic surveillance devices pose grave dangers to the privacy of all citizens of the commonwealth. Therefore, the secret use of such devices by private individuals must be prohibited. The use of such devices by law enforcement officials must be conducted under strict judicial supervision and should be limited to the investigation of organized crime.

B. Definitions. As used in this section—

1. The term "wire communication" means any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception.
2. The term "oral communication" means speech, except such speech as is transmitted over the public air waves by radio or other similar device.
3. The term "intercepting device" means any device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire or oral communication other than a hearing aid or similar device which is being used to correct subnormal hearing to normal and other than any telephone or telegraph instrument, equipment, facility, or a component thereof, (a) furnished to a subscriber or user by a communications common carrier in the ordinary course of its business under its tariff and being used by the

subscriber or user in the ordinary course of its business; or (b) being used by a communications common carrier in the ordinary course of its business.

4. The term "interception" means to secretly hear, secretly record, or aid 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; provided that it shall not constitute an interception for an investigative or law enforcement officer, as defined in this section, to record or transmit a wire or oral communication if the officer is a party to such communication or has been given prior authorization to record or transmit the communication by such a party and if recorded or transmitted in the course of an investigation of a designated offense as defined herein.

5. The term "contents", when used with respect to any wire or oral communication, means any information concerning the identity of the parties to such communication or the existence, contents, substance, purport, or meaning of that communication.

6. The term "aggrieved person" means any individual who was a party to an intercepted wire or oral communication or who was named in the warrant authorizing the interception, or who would otherwise have standing to complain that his personal or property interest or privacy was invaded in the course of an interception.

7. The term "designated offense" shall include the following offenses in connection with organized crime as defined in the preamble: arson, assault and battery with a dangerous weapon, extortion, bribery, burglary, embezzlement, forgery, gaming in violation of section seventeen of

chapter two hundred and seventy-one of the general laws, intimidation of a witness or juror, kidnapping, larceny, lending of money or things of value in violation of the general laws, mayhem, murder, any offense involving the possession or sale of a narcotic or harmful drug, perjury, prostitution, robbery, subornation of perjury, any violation of this section, being an accessory to any of the foregoing offenses and conspiracy or attempt or solicitation to commit any of the foregoing offenses.

8. The term "investigative or law enforcement officer" means any officer of the United States, a state or a political subdivision of a state, who is empowered by law to conduct investigations of, or to make arrests for, the designated offenses, and any attorney authorized by law to participate in the prosecution of such offenses.

9. The term "judge of competent jurisdiction" means any justice of the superior court of the commonwealth.

10. The term "chief justice" means the chief justice of the superior court of the commonwealth.

11. The term "issuing judge" means any justice of the superior court who shall issue a warrant as provided herein or in the event of his disability or unavailability any other judge of competent jurisdiction designated by the chief justice.

12. The term "communication common carrier" means any person engaged as a common carrier in providing or operating wire communication facilities.

13. The term "person" means any individual, partnership, association, joint stock company, trust, or corporation, whether or not any of the foregoing is an officer, agent or employee of the United States, a state, or

a political subdivision of a state.

14. The terms "sworn" or "under oath" as they appear in this section shall mean an oath or affirmation or a statement subscribed to under the pains and penalties of perjury.

15. The terms "applicant attorney general" or "applicant district attorney" shall mean the attorney general of the commonwealth or a district attorney of the commonwealth who has made application for a warrant pursuant to this section.

16. The term "exigent circumstances" shall mean the showing of special facts to the issuing judge as to the nature of the investigation for which a warrant is sought pursuant to this section which require secrecy in order to obtain the information desired from the interception sought to be authorized.

17. The term "financial institution" shall mean a bank, as defined in section 1 of chapter 167, and an investment bank, securities broker, securities dealer, investment adviser, mutual fund, investment company or securities custodian as defined in section 1.165-12(c)(1) of the United States Treasury regulations.

18. The term "corporate and institutional trading partners" shall mean financial institutions and general business entities and corporations which engage in the business of cash and asset management, asset management directed to custody operations, securities trading, and wholesale capital markets including foreign exchange, securities lending, and the purchase, sale or exchange of securities, options, futures, swaps, derivatives, repurchase agreements and other similar financial instruments with such financial institution.

C. Offenses.

1. Interception, oral communications prohibited.

Except as otherwise specifically provided in this section any person who

—
willfully commits an interception, attempts to commit an interception, or procures any other person to commit an interception or to attempt to commit an interception of any wire or oral communication shall be fined not more than ten thousand dollars, or imprisoned in the state prison for not more than five years, or imprisoned in a jail or house of correction for not more than two and one half years, or both so fined and given one such imprisonment.

Proof of the installation of any intercepting device by any person under circumstances evincing an intent to commit an interception, which is not authorized or permitted by this section, shall be prima facie evidence of a violation of this subparagraph.

2. Editing of tape recordings in judicial proceeding prohibited.

Except as otherwise specifically provided in this section any person who willfully edits, alters or tampers with any tape, transcription or recording of oral or wire communications by any means, or attempts to edit, alter or tamper with any tape, transcription or recording of oral or wire communications by any means with the intent to present in any judicial proceeding or proceeding under oath, or who presents such recording or permits such recording to be presented in any judicial proceeding or proceeding under oath, without fully indicating the nature of the changes made in the original state of the recording, shall be fined not more than

ten thousand dollars or imprisoned in the state prison for not more than five years or imprisoned in a jail or house of correction for not more than two years or both so fined and given one such imprisonment.

3. Disclosure or use of wire or oral communications prohibited.

Except as otherwise specifically provided in this section any person who

a. willfully discloses or attempts to disclose to any person the contents of any wire or oral communication, knowing that the information was obtained through interception; or

b. willfully uses or attempts to use the contents of any wire or oral communication, knowing that the information was obtained through interception, shall be guilty of a misdemeanor punishable by imprisonment in a jail or a house of correction for not more than two years or by a fine of not more than five thousand dollars or both.

4. Disclosure of contents of applications, warrants, renewals, and returns prohibited.

Except as otherwise specifically provided in this section any person who

willfully discloses to any person, any information concerning or contained in, the application for, the granting or denial of orders for interception, renewals, notice or return on an ex parte order granted pursuant to this section, or the contents of any document, tape, or recording kept in accordance with paragraph N, shall be guilty of a misdemeanor punishable by imprisonment in a jail or a house of correction for not more than two years or by a fine of not more than five thousand dollars or both.

5. Possession of interception devices prohibited.

A person who possesses any intercepting device under circumstances evincing an intent to commit an interception not permitted or authorized by this section, or a person who permits an intercepting device to be used or employed for an interception not permitted or authorized by this section, or a person who possesses an intercepting device knowing that the same is intended to be used to commit an interception not permitted or authorized by this section, shall be guilty of a misdemeanor punishable by imprisonment in a jail or house of correction for not more than two years or by a fine of not more than five thousand dollars or both.

The installation of any such intercepting device by such person or with his permission or at his direction shall be prima facie evidence of possession as required by this subparagraph.

6. Any person who permits or on behalf of any other person commits or attempts to commit, or any person who participates in a conspiracy to commit or to attempt to commit, or any accessory to a person who commits a violation of subparagraphs 1 through 5 of paragraph C of this section shall be punished in the same manner as is provided for the respective offenses as described in subparagraphs 1 through 5 of paragraph C.

D. Exemptions.

1. Permitted interception of wire or oral communications.

It shall not be a violation of this section—

a. for an operator of a switchboard, or an officer, employee, or agent of any communication common carrier, whose facilities are used in the transmission of a wire communication, to intercept, disclose, or use that

communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of service or to the protection of the rights or property of the carrier of such communication, or which is necessary to prevent the use of such facilities in violation of section fourteen A of chapter two hundred and sixty-nine of the general laws; provided, that said communication common carriers shall not utilize service observing or random monitoring except for mechanical or service quality control checks.

b. for persons to possess an office intercommunication system which is used in the ordinary course of their business or to use such office intercommunication system in the ordinary course of their business.

c. for investigative and law enforcement officers of the United States of America to violate the provisions of this section if acting pursuant to authority of the laws of the United States and within the scope of their authority.

d. for any person duly authorized to make specified interceptions by a warrant issued pursuant to this section.

e. for investigative or law enforcement officers to violate the provisions of this section for the purposes of ensuring the safety of any law enforcement officer or agent thereof who is acting in an undercover capacity, or as a witness for the commonwealth; provided, however, that any such interception which is not otherwise permitted by this section shall be deemed unlawful for purposes of paragraph P.

f. for a financial institution to record telephone communications with its corporate or institutional trading partners in the ordinary course of its business; provided, however, that such financial institution shall establish

and maintain a procedure to provide semi-annual written notice to its corporate and institutional trading partners that telephone communications over designated lines will be recorded.

2. Permitted disclosure and use of intercepted wire or oral communications.

a. Any investigative or law enforcement officer, who, by any means authorized by this section, has obtained knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may disclose such contents or evidence in the proper performance of his official duties.

b. Any investigative or law enforcement officer, who, by any means authorized by this section has obtained knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may use such contents or evidence in the proper performance of his official duties.

c. Any person who has obtained, by any means authorized by this section, knowledge of the contents of any wire or oral communication, or evidence derived therefrom, may disclose such contents while giving testimony under oath or affirmation in any criminal proceeding in any court of the United States or of any state or in any federal or state grand jury proceeding.

d. The contents of any wire or oral communication intercepted pursuant to a warrant in accordance with the provisions of this section, or evidence derived therefrom, may otherwise be disclosed only upon a showing of good cause before a judge of competent jurisdiction.

e. No otherwise privileged wire or oral communication intercepted in accordance with, or in violation of, the provisions of this section shall lose its privileged character.

E. Warrants: when issuable:

A warrant may issue only:

1. Upon a sworn application in conformity with this section; and
2. Upon a showing by the applicant that there is probable cause to believe that a designated offense has been, is being, or is about to be committed and that evidence of the commission of such an offense may thus be obtained or that information which will aid in the apprehension of a person who the applicant has probable cause to believe has committed, is committing, or is about to commit a designated offense may thus be obtained; and
3. Upon a showing by the applicant that normal investigative procedures have been tried and have failed or reasonably appear unlikely to succeed if tried.

F. Warrants: application.

1. Application. The attorney general, any assistant attorney general specially designated by the attorney general, any district attorney, or any assistant district attorney specially designated by the district attorney may apply ex parte to a judge of competent jurisdiction for a warrant to intercept wire or oral communications. Each application ex parte for a warrant must be in writing, subscribed and sworn to by the applicant authorized by this subparagraph.
2. The application must contain the following:
 - a. A statement of facts establishing probable cause to believe that a particularly described designated offense has been, is being, or is about to be committed; and

- b. A statement of facts establishing probable cause to believe that oral or wire communications of a particularly described person will constitute evidence of such designated offense or will aid in the apprehension of a person who the applicant has probable cause to believe has committed, is committing, or is about to commit a designated offense; and
- c. That the oral or wire communications of the particularly described person or persons will occur in a particularly described place and premises or over particularly described telephone or telegraph lines; and
- d. A particular description of the nature of the oral or wire communications sought to be overheard; and
- e. A statement that the oral or wire communications sought are material to a particularly described investigation or prosecution and that such conversations are not legally privileged; and
- f. A statement of the period of time for which the interception is required to be maintained. If practicable, the application should designate hours of the day or night during which the oral or wire communications may be reasonably expected to occur. If the nature of the investigation is such that the authorization for the interception should not automatically terminate when the described oral or wire communications have been first obtained, the application must specifically state facts establishing probable cause to believe that additional oral or wire communications of the same nature will occur thereafter; and
- g. If it is reasonably necessary to make a secret entry upon a private place and premises in order to install an intercepting device to effectuate the interception, a statement to such effect; and

h. If a prior application has been submitted or a warrant previously obtained for interception of oral or wire communications, a statement fully disclosing the date, court, applicant, execution, results, and present status thereof; and

i. If there is good cause for requiring the postponement of service pursuant to paragraph L, subparagraph 2, a description of such circumstances, including reasons for the applicant's belief that secrecy is essential to obtaining the evidence or information sought.

3. Allegations of fact in the application may be based either upon the personal knowledge of the applicant or upon information and belief. If the applicant personally knows the facts alleged, it must be so stated. If the facts establishing such probable cause are derived in whole or part from the statements of persons other than the applicant, the sources of such information and belief must be either disclosed or described; and the application must contain facts establishing the existence and reliability of any informant and the reliability of the information supplied by him. The application must also state, so far as possible, the basis of the informant's knowledge or belief. If the applicant's information and belief is derived from tangible evidence or recorded oral evidence, a copy or detailed description thereof should be annexed to or included in the application. Affidavits of persons other than the applicant may be submitted in conjunction with the application if they tend to support any fact or conclusion alleged therein. Such accompanying affidavits may be based either on personal knowledge of the affiant or information and belief, with the source thereof, and reason therefor, specified.

G. Warrants: application to whom made.

Application for a warrant authorized by this section must be made to a judge of competent jurisdiction in the county where the interception is to occur, or the county where the office of the applicant is located, or in the event that there is no judge of competent jurisdiction sitting in said county at such time, to a judge of competent jurisdiction sitting in Suffolk County; except that for these purposes, the office of the attorney general shall be deemed to be located in Suffolk County.

H. Warrants: application how determined.

1. If the application conforms to paragraph F, the issuing judge may examine under oath any person for the purpose of determining whether probable cause exists for the issuance of the warrant pursuant to paragraph E. A verbatim transcript of every such interrogation or examination must be taken, and a transcription of the same, sworn to by the stenographer, shall be attached to the application and be deemed a part thereof.
2. If satisfied that probable cause exists for the issuance of a warrant the judge may grant the application and issue a warrant in accordance with paragraph I. The application and an attested copy of the warrant shall be retained by the issuing judge and transported to the chief justice of the superior court in accordance with the provisions of paragraph N of this section.
3. If the application does not conform to paragraph F, or if the judge is not satisfied that probable cause has been shown sufficient for the issuance of a warrant, the application must be denied.

I. Warrants: form and content.

A warrant must contain the following:

1. The subscription and title of the issuing judge; and
 2. The date of issuance, the date of effect, and termination date which in no event shall exceed thirty days from the date of effect. The warrant shall permit interception of oral or wire communications for a period not to exceed fifteen days. If physical installation of a device is necessary, the thirty-day period shall begin upon the date of installation. If the effective period of the warrant is to terminate upon the acquisition of particular evidence or information or oral or wire communication, the warrant shall so provide; and
 3. A particular description of the person and the place, premises or telephone or telegraph line upon which the interception may be conducted; and
 4. A particular description of the nature of the oral or wire communications to be obtained by the interception including a statement of the designated offense to which they relate; and
 5. An express authorization to make secret entry upon a private place or premises to install a specified intercepting device, if such entry is necessary to execute the warrant; and
 6. A statement providing for service of the warrant pursuant to paragraph L except that if there has been a finding of good cause shown requiring the postponement of such service, a statement of such finding together with the basis therefor must be included and an alternative direction for deferred service pursuant to paragraph L, subparagraph 2.
- J. Warrants: renewals.

1. Any time prior to the expiration of a warrant or a renewal thereof, the applicant may apply to the issuing judge for a renewal thereof with respect to the same person, place, premises or telephone or telegraph line. An application for renewal must incorporate the warrant sought to be renewed together with the application therefor and any accompanying papers upon which it was issued. The application for renewal must set forth the results of the interceptions thus far conducted. In addition, it must set forth present grounds for extension in conformity with paragraph F, and the judge may interrogate under oath and in such an event a transcript must be provided and attached to the renewal application in the same manner as is set forth in subparagraph 1 of paragraph H.

2. Upon such application, the judge may issue an order renewing the warrant and extending the authorization for a period not exceeding fifteen (15) days from the entry thereof. Such an order shall specify the grounds for the issuance thereof. The application and an attested copy of the order shall be retained by the issuing judge to be transported to the chief justice in accordance with the provisions of subparagraph N of this section. In no event shall a renewal be granted which shall terminate later than two years following the effective date of the warrant.

K. Warrants: manner and time of execution.

1. A warrant may be executed pursuant to its terms anywhere in the commonwealth.

2. Such warrant may be executed by the authorized applicant personally or by any investigative or law enforcement officer of the commonwealth designated by him for the purpose.

3. The warrant may be executed according to its terms during the hours specified therein, and for the period therein authorized, or a part thereof. The authorization shall terminate upon the acquisition of the oral or wire communications, evidence or information described in the warrant. Upon termination of the authorization in the warrant and any renewals thereof, the interception must cease at once, and any device installed for the purpose of the interception must be removed as soon thereafter as practicable. Entry upon private premises for the removal of such device is deemed to be authorized by the warrant.

L. Warrants: service thereof.

1. Prior to the execution of a warrant authorized by this section or any renewal thereof, an attested copy of the warrant or the renewal must, except as otherwise provided in subparagraph 2 of this paragraph, be served upon a person whose oral or wire communications are to be obtained, and if an intercepting device is to be installed, upon the owner, lessee, or occupant of the place or premises, or upon the subscriber to the telephone or owner or lessee of the telegraph line described in the warrant.

2. If the application specially alleges exigent circumstances requiring the postponement of service and the issuing judge finds that such circumstances exist, the warrant may provide that an attested copy thereof may be served within thirty days after the expiration of the warrant or, in case of any renewals thereof, within thirty days after the expiration of the last renewal; except that upon a showing of important special facts which set forth the need for continued secrecy to the satisfaction of the issuing judge, said judge may direct that the attested copy of the warrant be served on such parties as are required by this

section at such time as may be appropriate in the circumstances but in no event may he order it to be served later than three (3) years from the time of expiration of the warrant or the last renewal thereof. In the event that the service required herein is postponed in accordance with this paragraph, in addition to the requirements of any other paragraph of this section, service of an attested copy of the warrant shall be made upon any aggrieved person who should reasonably be known to the person who executed or obtained the warrant as a result of the information obtained from the interception authorized thereby.

3. The attested copy of the warrant shall be served on persons required by this section by an investigative or law enforcement officer of the commonwealth by leaving the same at his usual place of abode, or in hand, or if this is not possible by mailing the same by certified or registered mail to his last known place of abode. A return of service shall be made to the issuing judge, except, that if such service is postponed as provided in subparagraph 2 of paragraph L, it shall be made to the chief justice. The return of service shall be deemed a part of the return of the warrant and attached thereto.

M. Warrant: return.

Within seven days after termination of the warrant or the last renewal thereof, a return must be made thereon to the judge issuing the warrant by the applicant therefor, containing the following:

- a. a statement of the nature and location of the communications facilities, if any, and premise or places where the interceptions were made; and
- b. the periods of time during which such interceptions were made; and

- c. the names of the parties to the communications intercepted if known; and
- d. the original recording of the oral or wire communications intercepted, if any; and
- e. a statement attested under the pains and penalties of perjury by each person who heard oral or wire communications as a result of the interception authorized by the warrant, which were not recorded, stating everything that was overheard to the best of his recollection at the time of the execution of the statement.

N. Custody and secrecy of papers and recordings made pursuant to a warrant.

1. The contents of any wire or oral communication intercepted pursuant to a warrant issued pursuant to this section shall, if possible, be recorded on tape or wire or other similar device. Duplicate recordings may be made for use pursuant to subparagraphs 2 (a) and (b) of paragraph D for investigations. Upon examination of the return and a determination that it complies with this section, the issuing judge shall forthwith order that the application, all renewal applications, warrant, all renewal orders and the return thereto be transmitted to the chief justice by such persons as he shall designate. Their contents shall not be disclosed except as provided in this section. The application, renewal applications, warrant, the renewal order and the return or any one of them or any part of them may be transferred to any trial court, grand jury proceeding of any jurisdiction by any law enforcement or investigative officer or court officer designated by the chief justice and a trial justice may allow them to be disclosed in accordance with paragraph D, subparagraph 2, or paragraph O or any other applicable provision of this section.

The application, all renewal applications, warrant, all renewal orders and the return shall be stored in a secure place which shall be designated by the chief justice, to which access shall be denied to all persons except the chief justice or such court officers or administrative personnel of the court as he shall designate.

2. Any violation of the terms and conditions of any order of the chief justice, pursuant to the authority granted in this paragraph, shall be punished as a criminal contempt of court in addition to any other punishment authorized by law.

3. The application, warrant, renewal and return shall be kept for a period of five (5) years from the date of the issuance of the warrant or the last renewal thereof at which time they shall be destroyed by a person designated by the chief justice. Notice prior to the destruction shall be given to the applicant attorney general or his successor or the applicant district attorney or his successor and upon a showing of good cause to the chief justice, the application, warrant, renewal, and return may be kept for such additional period as the chief justice shall determine but in no event longer than the longest period of limitation for any designated offense specified in the warrant, after which time they must be destroyed by a person designated by the chief justice.

O. Introduction of evidence.

1. Notwithstanding any other provisions of this section or any order issued pursuant thereto, in any criminal trial where the commonwealth intends to offer in evidence any portions of the contents of any interception or any evidence derived therefrom the defendant shall be served with a complete copy of each document and item which make up each application, renewal application, warrant, renewal order, and return

pursuant to which the information was obtained, except that he shall be furnished a copy of any recording instead of the original. The service must be made at the arraignment of the defendant or, if a period in excess of thirty (30) days shall elapse prior to the commencement of the trial of the defendant, the service may be made at least thirty (30) days before the commencement of the criminal trial. Service shall be made in hand upon the defendant or his attorney by any investigative or law enforcement officer of the commonwealth. Return of the service required by this subparagraph including the date of service shall be entered into the record of trial of the defendant by the commonwealth and such return shall be deemed prima facie evidence of the service described therein. Failure by the commonwealth to make such service at the arraignment, or if delayed, at least thirty days before the commencement of the criminal trial, shall render such evidence illegally obtained for purposes of the trial against the defendant; and such evidence shall not be offered nor received at the trial notwithstanding the provisions of any other law or rules of court.

2. In any criminal trial where the commonwealth intends to offer in evidence any portions of a recording or transmission or any evidence derived therefrom, made pursuant to the exceptions set forth in paragraph B, subparagraph 4, of this section, the defendant shall be served with a complete copy of each recording or a statement under oath of the evidence overheard as a result of the transmission. The service must be made at the arraignment of the defendant or if a period in excess of thirty days shall elapse prior to the commencement of the trial of the defendant, the service may be made at least thirty days before the commencement of the criminal trial. Service shall be made in hand upon the defendant or his attorney by any investigative or law enforcement officer of the commonwealth. Return of the service required by this subparagraph

including the date of service shall be entered into the record of trial of the defendant by the commonwealth and such return shall be deemed prima facie evidence of the service described therein. Failure by the commonwealth to make such service at the arraignment, or if delayed at least thirty days before the commencement of the criminal trial, shall render such service illegally obtained for purposes of the trial against the defendant and such evidence shall not be offered nor received at the trial notwithstanding the provisions of any other law or rules of court.

P. Suppression of evidence.

Any person who is a defendant in a criminal trial in a court of the commonwealth may move to suppress the contents of any intercepted wire or oral communication or evidence derived therefrom, for the following reasons:

1. That the communication was unlawfully intercepted.
2. That the communication was not intercepted in accordance with the terms of this section.
3. That the application or renewal application fails to set forth facts sufficient to establish probable cause for the issuance of a warrant.
4. That the interception was not made in conformity with the warrant.
5. That the evidence sought to be introduced was illegally obtained.
6. That the warrant does not conform to the provisions of this section.

Q. Civil remedy.

Any aggrieved person whose oral or wire communications were intercepted, disclosed or used except as permitted or authorized by this section or whose personal or property interests or privacy were violated

by means of an interception except as permitted or authorized by this section shall have a civil cause of action against any person who so intercepts, discloses or uses such communications or who so violates his personal, property or privacy interest, and shall be entitled to recover from any such person—

1. actual damages but not less than liquidated damages computed at the rate of \$100 per day for each day of violation or \$1000, whichever is higher;
2. punitive damages; and
3. a reasonable attorney's fee and other litigation disbursements reasonably incurred. Good faith reliance on a warrant issued under this section shall constitute a complete defense to an action brought under this paragraph.

R. Annual report of interceptions of the general court.

On the second Friday of January, each year, the attorney general and each district attorney shall submit a report to the general court stating (1) the number of applications made for warrants during the previous year, (2) the name of the applicant, (3) the number of warrants issued, (4) the effective period for the warrants, (5) the number and designation of the offenses for which those applications were sought, and for each of the designated offenses the following: (a) the number of renewals, (b) the number of interceptions made during the previous year, (c) the number of indictments believed to be obtained as a result of those interceptions, (d) the number of criminal convictions obtained in trials where interception evidence or evidence derived therefrom was introduced. This report shall be a public document and be made available to the public at the offices of

the attorney general and district attorneys. In the event of failure to comply with the provisions of this paragraph any person may compel compliance by means of an action of mandamus.

CERTIFICATE OF COMPLIANCE

I David Quinn Gacioch 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 application 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 point, and contains 10,993, total non-excluded words as counted using the word count feature of Microsoft Word (Microsoft Office 2016 edition).

/s/ David Quinn Gacioch

David Quinn Gacioch, BBO No. 660784

McDERMOTT WILL & EMERY LLP

200 Clarendon Street, Floor 58

Boston, MA 02116

(617) 535-4000

dgacioch@mwe.com

CERTIFICATE OF SERVICE

Pursuant to Mass. R. A. P. 13(d), I hereby certify, under the penalties of perjury, that on February 7, 2024 I have made service of this Brief and Appendices upon the attorney of record for each party, by email and the Electronic Filing System on:

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

/s/ David Quinn Gacioch
David Quinn Gacioch, BBO No. 660784
MCDERMOTT WILL & EMERY LLP
200 Clarendon Street, Floor 58
Boston, MA 02116
(617) 535-4000
dgacioch@mwe.com