No. SJC-13542

COMMONWEALTH OF MASSACHUSETTS
SUPREME JUDICIAL COURT

Kathleen Vita,

Plaintiff-Appellee,

v.

New England Baptist Hospital and *Beth Israel Deaconess Medical Center, Inc.*,

Defendants-Appellants.

Reported to the Appeals Court from the Superior Court
Direct Appellate Review Granted

BRIEF OF *AMICUS CURIAE* THE CHAMBER OF COMMERCE OF THE UNITED STATES OF AMERICA IN SUPPORT OF REVERSAL

Emily Johnson Henn (*pro hac vice pending*)
COVINGTON & BURLING LLP
3000 El Camino Real
5 Palo Alto Square, 10th Floor
Palo Alto, CA 94306
Telephone: (650) 632-4700

Geoffrey Hobart, BBO No. 547499
COVINGTON & BURLING LLP
One International Place
Suite 1020
Boston, MA 02110
Telephone: (617) 603-8800

Mark W. Mosier (*pro hac vice pending*)
Michael M. Maya, BBO No. 672847
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001
Telephone: (202) 662-6000

Counsel for the Chamber of Commerce of the United States of America

CORPORATE DISCLOSURE STATEMENT

Pursuant to Massachusetts Appellate Procedure Rule 17(c)(1) and Supreme Judicial Court Rule 1:21, the Chamber of Commerce of the United States of America (the "Chamber") states that it has no parent corporation. No publicly held corporation owns any portion of the Chamber, and the Chamber is neither a subsidiary nor an affiliate of any publicly owned corporation.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTEREST OF *AMICUS CURIAE*

Pursuant to Massachusetts Appellate Procedure Rule 17, the Chamber of Commerce of the United States of America (the "Chamber") submits this brief *amicus curiae* in support of reversal.

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

The Chamber's members have websites that are accessible in Massachusetts and many of them use website analytics tools like those at issue in this case. The members of the Chamber have a fundamental interest in providing information and conducting transactions via their websites without fear of crippling and virtually unlimited liability under the Massachusetts Wiretap Act.

PREPARATION OF AMICUS BRIEF

Pursuant to Massachusetts Appellate Procedure Rule 17(c)(5), amicus and counsel declare that:

(a) no party or party's counsel authored the brief in whole or in part;

(b) no party or party's counsel, or any other person or entity, other than the Chamber, its members, or its counsel, contributed money that was intended to fund the preparation or submission of this brief; and

(c) counsel has not represented any party in this case or any party in a proceeding involving similar issues.

INTRODUCTION AND SUMMARY OF ARGUMENT

Plaintiff in these cases asserts claims that are becoming increasingly common in courts across the United States. A plaintiff visits a website that uses analytics tools—*i.e.*, third-party software—to collect data about how the visitor uses the site. The plaintiff does not allege that the website or the analytics tools collected their private or sensitive information, or that they suffered any actual harm based on the collection of their clicks, scrolls, and other movements on the website. The plaintiff nevertheless alleges a violation of a state wiretap law and seeks statutory penalties or liquidated damages.

Hundreds of these cases are currently pending in state and federal courts across the country, including at least twenty in Massachusetts. Nationwide, some courts have dismissed similar claims for lack of standing, given that the plaintiff alleges no actual injury; other courts have dismissed for lack of personal jurisdiction when the suit is not brought where the defendant resides or the challenged conduct took place; still others have dismissed for failure to state a claim.[1]

[1] *See, e.g.*, *Adams v. PSP Grp., LLC*, __ F. Supp. 3d __, 2023 WL 5951784, at *1 (E.D. Mo. Sept. 13, 2023) (dismissing for lack of standing), *appeal docketed*, No. 23-3303 (8th Cir. Oct. 17, 2023); *Massie v. Gen. Motors Co.*, No. 1:20-CV-01560-JLT, 2021 WL 2142728, at *1 (E.D. Cal. May 26, 2021) (dismissing for lack of personal jurisdiction); *Goldstein v. Costco Wholesale Corp.*, 559 F. Supp. 3d 1318, 1319 (S.D. Fla. 2021) (dismissing for failure to state a claim).

If allowed to stand, the Superior Court's rulings in these cases would reverse that trend. The court held that a plaintiff need not allege an actual injury to have standing and that a plaintiff can state a claim by alleging that a website used the most popular website analytics tools—Google Analytics and Meta Pixel—to collect the plaintiff's clicks and scrolls on the website. There is virtually no limit on the number of cases that could be brought under this theory. Google Analytics and Meta Pixel are used on roughly fifty million websites, and many of the sites using these tools can be identified through a simple Google search. As a result, in an hour or two of web surfing, a single would-be plaintiff could manufacture injury-less claims against hundreds, if not thousands, of defendants.

That result can easily be avoided through a proper interpretation of the Massachusetts Wiretap Act, G.L. c. 262, § 99 ("Wiretap Act"). When the legislature enacted the relevant provisions in 1968, it sought to prohibit the use of physical devices to intercept conversations. The language it used in that statute cannot reasonably be read to prohibit businesses from using analytics tools to track how their websites are used.

I. Plaintiff's claims would harm businesses by exposing them to massive liability for using industry-standard website analytics tools. Millions of companies use website analytics tools because they improve the user experience on their websites. These tools help businesses design more user-friendly websites, detect fraud, and

increase the likelihood that users see advertising that is relevant to them. Those benefits may be lost if Plaintiff's claims are allowed to continue. Under Plaintiff's theory, each website visit would expose the website operator to $1,000 in liquidated damages. With even a moderate amount of website traffic, a company's potential exposure could reach into the millions, if not billions, of dollars. Businesses will be forced to consider changing how and whether they use analytics tools at all given the potential for ruinous liability.

II. The Wiretap Act does not prohibit the use of website analytics tools because, among other reasons, those tools neither use an "intercepting device" nor intercept "wire communications." An "intercepting device" is a tangible object—a physical piece of equipment—not intangible computer code. And even if computer code embedded in websites could be a device, the Wiretap Act still would not cover website analytics tools because they are used in the ordinary course of business. Moreover, Plaintiff's Wiretap Act claims must fail because she has not alleged that any "communications" were intercepted—collecting data on website clicks and scrolls is not enough. Rather than rewriting the statute to cover use of data analytics tools, the Court should interpret the statute as written and leave to the legislature the decision whether to amend the statute to address such tools.

In sum, businesses do not violate the Wiretap Act when they use website analytics tools to collect data on how visitors use their websites. The Superior Court's

decisions misinterpret the law, would lead to an explosion of unwarranted litigation, and should be reversed.

ARGUMENT

I. The Superior Court's Rulings Discourage the Use of Beneficial, Industry-Standard Website Analytics Tools By Exposing Businesses to Potentially Massive Liability for Using Them.

The Superior Court's rulings expose businesses that operate websites—which is virtually every business—to potentially crippling liability for using website analytics tools. Businesses use these industry-standard tools to design more user-friendly websites, detect fraud, and deliver more relevant advertising. Businesses and consumers would be harmed by the de facto ban that would result from upholding the Superior Court's rulings.

A. Website Analytics Tools Are Widely Used Because They Help Businesses Serve Their Customers.

"Web analytics is the collection, measurement, analysis, and reporting of digital data to enhance insights concerning the behavior of website visitors."[2] Website analytics tools are widely used by every type of website operator—from Fortune 500 companies to government agencies—because they help provide a better experience

[2] *See* Bernard J. Jansen et al., *Measuring User Interactions with Websites: A Comparison of Two Industry Standard Analytics Approaches Using Data of 86 Websites*, 17(5) PLoS One e0268212, at 1–3 (May 27, 2022), https://doi.org/10.1371/journal.pone.0268212 (describing Google Analytics as "the industry-standard website analytics platform").

for visitors to the website. As the U.S. General Services Administration ("GSA") has observed, "[g]athering and analyzing metrics and data on how people use your website can help you make design and development decisions informed by data, rather than by guess or executive whim."[3]

Website analytics tools lead to more efficient and effective customer experiences by "provid[ing] the website owner with insights about how users use the website, which the owner can use to improve the website." R:A:I:17 & R:A:IV:18 (¶ 37). Businesses typically seek "clarity, simplicity, and consistency in web design so that users can perform desired operations efficiently and effectively. If a website lacks these characteristics, users may become confused or frustrated and 'take their business' to competing sites."[4] Website analytics tools can provide insight into whether a website is operating efficiently and effectively or whether customers grow frustrated with the site and leave without making a purchase. For example, statistics

[3] *An Introduction to Analytics*, Digital.gov, https://perma.cc/UYL8-LPUB (archived Mar. 11, 2024).

[4] James J. Cappel & Zhenyu Huang, *A Usability Analysis of Company Websites*, 48(1) J. Comput. Info. Sys. 117, 117 (2007).

such as a "bounce rate" can signal to a business that its website is not meeting visitors' needs.[5]

Website analytics tools also help businesses detect fraud. "By analyzing large volumes of transactional and behavioral data, data analytics techniques can detect deviations from normal patterns, highlight suspicious activities, and pinpoint potential instances of fraud."[6] For example, website analytics can quickly identify credit card fraud by detecting "if a credit card is suddenly used for transactions in different geographical locations within a short time span."[7] Likewise, website analytics tools can uncover identity theft "[b]y analyzing login patterns, geographic locations, and device usage."[8] These fraud detection tools are not used solely for the benefit of the website operator. Customers whose credit cards or identities have been stolen also benefit from websites detecting and deterring that fraudulent activity.

---

[5] The term "bounce rate" refers to the rate at which "a user who has visited the website leaves without interacting with it." *See What Is Web Analytics and Its 10 Benefits*, Engaio Digital, https://perma.cc/Y75Q-UC3F (archived Mar. 11, 2024). "A high bounce rate" can mean that "[t]he users didn't feel that content was for them," or it could reflect "[a] weak user experience overall." *Id.*; *see also* Jansen et al., *supra*, at 6 n.2 (noting "bounce rates . . . may indicate a lack of engagement").

[6] *Fraud Detection Through Data Analytics: Identifying Anomalies and Patterns*, Int'l Ass'n of Bus. Analytics Certification (Sept. 20, 2023), https://perma.cc/375C-377T.

[7] *Id.*

[8] *Id.*

Plaintiff alleges that websites can use data analytics "to serve . . . individuals with better-targeted individualized advertisements." R:A:I:17 & R:A:IV:18 (¶ 37). That is true, but Plaintiff is wrong to suggest that targeted advertising benefits only the online seller. Targeted advertising can benefit consumers by: (i) making the shopping experience more efficient; (ii) introducing them to new brands or products that are more likely to interest them; (iii) offering sales and other promotional incentives; and (iv) promoting local businesses.[9] Indeed, in a recent survey, more than half of the respondents identified one of these benefits of targeted advertising.[10] Without data for personalized advertising, businesses and other advertisers "cannot show the right ad to the right user, [and] consumers are the ultimate losers," as businesses' "revenues will plummet, and consumers will no longer receive the free apps and services that advertising makes possible."[11]

---

[9] Press Release, Visual Objects, *Despite Negative Perceptions, 52% of Consumers Can Identify Benefits of Targeted Advertising*, PR Newswire (Mar. 25, 2021), https://perma.cc/QB9D-B88S.

[10] *Id.*

[11] D. Daniel Sokol & Feng Zhu, Essay, *Harming Competition and Consumers Under the Guise of Protecting Privacy: An Analysis of Apple's iOS 14 Policy Updates*, 107 Cornell L. Rev. Online 94, 98, 100 (2022) (also stating, "The ad-supported model has enabled the open internet to flourish, and impacts the financial viability of . . . entire sectors."); *see also* Ashley Johnson, *Banning Targeted Ads Would Sink the Internet Economy*, Info. Tech. & Innovation Found. (Jan. 20, 2022), https://perma.cc/5TAG-9KPZ ("In a world without targeted advertising, or where targeted advertising is less effective due to excessive restrictions on data collection and use, many websites or apps would earn less revenue. This would mean they (continued…)

Website analytics tools may be relatively new, but they largely seek to implement the same practices that businesses have long used in their brick-and-mortar stores. Shopkeepers have long sought to organize and arrange their stores to make the shopping experience more convenient for customers. They use security cameras to detect fraud and deter shoplifting. And they promote selected products to their customers by putting them on display near the front of the store or by cash registers.

The similarities between the information collected from websites and brick-and-mortar shoppers have not gone unnoticed. As one court observed in a suit brought against a video-game retailer,

> [Website analytics] information is no different from what GameStop employees would have been able to observe if Ms. Cook had gone into a brick-and-mortar store and began browsing the inventory. Her physical movements in the store are like her mouse movements, her pauses to look at inventory are like her mouse pointer hovering over products, and her picking up video games off the shelf are like placing those same titles in her virtual cart. Ms. Cook certainly doesn't have a reasonable expectation of privacy in this kind of public shopping behavior in the physical world, and she doesn't have it in the digital world, either.

---

have to start charging users fees or increase what they already charge for their services.").

Cook v. GameStop, Inc., __ F. Supp. 3d __, 2023 WL 5529772, at *5 (W.D. Pa. Aug. 28, 2023), *appeal docketed*, No. 23-2574 (3d Cir. Aug. 29, 2023).[12]

B. The Superior Court's Rulings Threaten Businesses with Crippling Liability for Using Website Analytics Tools.

Despite the widespread and beneficial use of website analytics tools, Plaintiff contends that those tools unlawfully intercept wire communications in violation of the Massachusetts Wiretap Act. R:A:I:55–56 (¶¶ 118–122); R:A:IV:49–50 (¶¶ 108–112). In Plaintiff's view, any person who visits a website using analytics tools is entitled to at least $1,000 in liquidated damages. R:A:I:56 (¶ 123); R:A:IV:51 (¶ 113). If that were correct, businesses would face crippling penalties.

Plaintiff's theory would expose as many as fifty million website operators to liability.[13] Plaintiff alleges Wiretap Act violations based on the Defendant-Hospitals' use of Google Analytics and Meta Pixel. R:A:I:55–56 (¶¶ 119–121);

[12] *See also Farst v. AutoZone, Inc.*, __ F. Supp. 3d __, 2023 WL 7179807, at *5 (M.D. Pa. Nov. 1, 2023) (plaintiff's "interactions with [defendant's] website might reveal some of his shopping preferences and habits, but that is akin to what would be revealed during a visit to [defendant's] brick and mortar store." (cleaned up)); *Goldstein*, 559 F. Supp. 3d at 1321 ("[T]his mere tracking of Plaintiff's movements on Defendant's website is the cyber analog to record information Defendant could have obtained through a security camera at a brick-and-mortar store.").

[13] Christopher Mims, *Who Has More of Your Personal Data Than Facebook? Try Google*, Wall St. J. (Apr. 22, 2018), https://www.wsj.com/articles/who-has-more-of-your-personal-data-than-facebook-try-google-1524398401 (explaining that, as of 2018, Google Analytics was "used on the sites of about half of the biggest companies in the U.S." and "has a total reach of 30 million to 50 million sites").

R:A:IV:49–50 (¶¶ 109–112). Google Analytics is the "most popular site analytics tool in use."[14] One recent survey estimated that roughly 53% of all websites use Google Analytics.[15] The same survey concluded that Meta Pixel was used on roughly 11% of all websites, making it the second-most used analytics tool.[16] Another survey estimated that "about 38 million websites use Google Analytics."[17]

Plaintiff's theory extends not only to commercial websites, but also to many government-operated sites. For example, the official website of the Commonwealth of Massachusetts, http://mass.gov, states that it "uses data analytics and interactive tools to make the site more responsive to customer needs."[18] The website identifies more than a dozen analytics tools that it uses, including both Google Analytics and Facebook Pixel.[19] With respect to the federal government, the GSA operates "a unified Google Analytics account for U.S. federal government agencies," which currently includes "more than 500 federal government second level domains . . . ,

---

[14] *See* Jansen et al., *supra*, at 6 n.2 (describing Google Analytics as "the industry-standard website analytics platform").

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

[16] *Id.*

[17] *See* Jack Shepherd, *15 Essential Google Analytics Statistics You Need to Know in 2024*, Social Shepherd (Feb. 26, 2024), https://perma.cc/Z2MK-DRGV.

[18] *Third-Party Data Analytic Tools*, Mass.gov, https://perma.cc/AUH7-U5SP (archived Mar. 11, 2024).

[19] *Id.*

including every executive branch cabinet department."[20] To encourage federal agencies to use Google Analytics, the GSA has set up a website, http://digital.gov, with information about how website analytics tools can improve the user experience.

Plaintiff's theory not only threatens tens of millions of businesses, non-profits, and other website operators with liability, but it threatens them with tens of millions of dollars in penalties, if not more. A business or organization using an analytics tool like Google Analytics could incur $1,000 in liability for every visitor to its website. G.L. c. 272, § 99(Q)(1). Indeed, applying the Wiretap Act to web analytics tools could cripple businesses big and small. For example, a small business with 5,000 monthly website visits could incur $60 million in damages over the course of a year.[21] These penalties would bankrupt most small businesses several times over without plaintiffs needing to show any injury.

Plaintiffs may attempt to downplay the threat of liability by arguing that a business can avoid liability under the Wiretap Act by obtaining a visitor's consent to collecting their browsing information. But that is cold comfort for businesses because plaintiffs often also challenge the adequacy of the notice a website provides

[20] Homepage, Analytics.usa.gov, https://perma.cc/7KZC-LVPG (archived Mar. 11, 2024).

[21] *See* Anna Fitzgerald, *How Many Visitors Should Your Website Get? [Data from 400+ Web Traffic Analysts]*, HubSpot (June 19, 2023), https://perma.cc/3EG8-HWBE (showing that nearly three-quarters of small businesses with 11 to 25 employees receive 1,001 to 15,000 monthly visits).

to its users about its use of analytics tools.[22] Plaintiffs also often argue that the adequacy of notice and consent presents questions of fact that cannot be resolved on a motion to dismiss.[23] As a result, even if a plaintiff's claims may ultimately lack merit, they impose substantial litigation costs and put pressure on a defendant to settle. That is especially true when, as is often the case, a plaintiff brings their claims as a putative class action. *See, e.g.*, *AT&T Mobility LLC v. Concepcion*, 563 U.S. 333, 350 (2011) (putative class actions present a significant "risk of 'in terrorem' settlements," because defendants "[f]aced with even a small chance of a devastating loss . . . will be pressured into settling questionable claims").

The Partners Healthcare settlement provides a good example. There, a hospital paid $18.4 million to settle claims like those brought here once they

[22] For example, Plaintiff alleges that the Defendant-Hospitals' websites provide insufficient notice of their use of analytics tools in these cases. R:A:I:13–14 & R:A:IV:14–15 (¶ 22–24); *see also, e.g.*, *Vonbergen v. Liberty Mut. Ins. Co.*, No. CV 22-4880, 2023 WL 8569004, at *12 (E.D. Pa. Dec. 11, 2023) (plaintiff alleging that she "was not presented with any type of pop-up disclosure or consent form"); *Yoon v. Lululemon USA, Inc.*, 549 F. Supp. 3d 1073, 1081 (C.D. Cal. 2021) (plaintiff alleging that she did not consent where the website did not "prompt[] [users] to take any affirmative action to demonstrate assent").

[23] For example, Plaintiff has so argued in these cases. R:A:I:124; R:A:IV:115–16; *see also, e.g.*, *Yoon*, 549 F. Supp. 3d at 1081 (declining to decide whether plaintiff consented to the data collection at the motion to dismiss stage).

survived an initial motion to dismiss.[24] Many putative class actions alleging Wiretap Act violations based on use of web analytics software were filed in quick succession following the Partners settlement.[25] If the Superior Court's decisions are affirmed, plaintiffs can be expected to bring suits against even more defendants. And those defendants will feel pressure to settle those claims for significant amounts of money, just as Partners did. Those businesses will also feel pressure to change how they use website analytics tools—despite their many benefits—to avoid incurring additional liability in the future, harming businesses and consumers. The Court can avoid that result—and ensure that businesses and government agencies can continue to use website analytics tools—by properly interpreting the Wiretap Act not to prohibit use of those tools.

[24] Steve Alder, *Mass General Brigham Settles 'Cookies Without Consent' Lawsuit for $18.4 Million*, HIPAA J. (Jan. 20, 2022), https://www.hipaajournal.com/mass-general-brigham-settles-cookies-without-consent-lawsuit-for-18-4-million/; *see also* Tr. of Rule 12 Hearing, *Doe v. Partners Healthcare Sys., Inc.*, No. 1984CV01651-BLS-1 (Mass. Super. Ct. Nov. 20, 2020); R:A:II:32–119 (Endorsed Order Allowing in Part and Denying in Part Motion to Dismiss); R:A:II:27. Partners Healthcare is now called Mass General Brigham. Alder, *Mass General Settles*, *supra*.

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

II. The Wiretap Act Does Not Prohibit the Use of Website Analytics Tools.

The Wiretap Act's text, context, and history demonstrate that the Massachusetts legislature did not intend the statute to prohibit a business from collecting data on how visitors use its website. Plaintiff has not alleged a violation of the Wiretap Act because, among other things, she does not adequately allege that the website analytics tools use an "intercepting device" or intercept "wire communications."

A. The Website Analytics Tools Did Not Use an "Intercepting Device."

The Wiretap Act defines "intercepting device" as "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[.]" G.L. c. 272, § 99(B)(3). This statutory definition expressly excludes "any telephone or telegraph instrument, equipment, facility, or a component thereof . . . being used by a communications common carrier in the ordinary course of its business." *Id.*

Plaintiff contends that website analytics tools use an "intercepting device," because they require snippets of computer code to be embedded on a website. That interpretation fails for two independent reasons. *First*, an intercepting device is a tangible object—a physical piece of equipment—not intangible computer code. *Second*, website analytics code is excluded from the statutory definition because it is used in the ordinary course of business.

1. Computer Code Is Not a Device.

Plaintiff's attempt to prohibit the use of website analytics tools depends on

her view that snippets of computer code constitute an "intercepting device." G.L. c. 272, § 99. The statutory text, context, and purpose refute that view.

The statutory text establishes that a "device" is a tangible item. This Court "determine[s] a word's usual and accepted meanings from sources presumably known to the statute's enactors, such as dictionary definitions." *Ortiz v. Examworks, Inc.*, 470 Mass. 784, 788 (2015) (cleaned up). When the Wiretap Act was enacted, the terms "device" and "apparatus" both referred to a piece of equipment: "device" meant "a piece of equipment or a mechanism designed to serve a special purpose or perform a special function," while an "apparatus" was "a set of materials or equipment designed for a particular use." *Webster's Seventh New Collegiate Dictionary* 42, 227 (1967). Those common definitions cannot be read to include lines of computer code embedded on a website.

Other provisions of the Wiretap Act confirm that the legislature was focused on the use of physical devices to overhear conversations. The statute prohibits "[p]ossession of interception devices." G.L. c. 272, § 99(C)(5). A prohibition on possession makes sense as a way to regulate use of a physical item, but not as a way to prohibit computer programmers from drafting certain types of code. Similarly, the statute includes extensive and detailed provisions for the application and use of warrants for intercepting devices and allows for the "secret entry upon a private place and premises in order to install an intercepting device." *Id.* § 99(F)(2)(g). If a

warrant issues and an intercepting device must be installed, there must be notice "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." *Id.* § 99(L)(1). Statutory provisions addressing entry onto private property and notice to a property owner similarly contemplate placement of a physical device in a particular location—not embedded computer code on a website.

This interpretation is consistent with the history and purpose of the Wiretap Act. In the 1960s, the legislature was "[a]larmed by the commercial availability of sophisticated surveillance devices and the ease with which they facilitated surreptitious recording of private citizens," and thus "appointed a special commission in 1964 to investigate electronic eavesdropping." *Commonwealth v. Tavares*, 459 Mass. 289, 294–95 (2011). The 1967 interim report of the commission discussed the "availability of instruments for overhearing secretly private conversations." Interim Report of the Special Commission on Electronic Eavesdropping, S. No. 1469, at 2 (Ma. 1967). The instruments that existed at the time were things like bugs—"subminiature transmitters" that "could eavesdrop on unknowing speakers and transmit a very clear signal at least seven blocks in downtown Boston and could pick up a whisper at twenty feet." *Commonwealth v. Rainey*, 491 Mass. 632, 645 (2023) (cleaned up). Neither the legislature nor the commission contemplated the use of an intangible item like computer code to

intercept online activity.

Courts interpreting similar statutes have held that "software is not a 'device' under its plain meaning." *See United States v. Ackies*, 918 F.3d 190, 199 n.5 (1st Cir. 2019); *see also Jacome v. Spirit Airlines Inc.*, No. 2021-000947-CA-01, 2021 WL 3087860, at *5 (Fla. Cir. Ct. June 17, 2021) (observing that "courts have held that software . . . [does] not constitute [a] device[] under the wiretapping statutes"); *Connor v. Whirlpool Corp.*, No. 21-CV-14180-WPD, 2021 WL 3076477, at *2 (S.D. Fla. July 6, 2021) (agreeing with *Jacome*); *Potter v. Havlicek*, No. 3:06-CV-211, 2008 WL 2556723, at *8 (S.D. Ohio June 23, 2008) (software is not a "device").

Interpreting "intercepting device" to include website code also leads to the anomalous result that the entire website is such a device. There is no meaningful difference between the JavaScript and HTML code used to collect a user's interactions with a website for use by analytics tools and the JavaScript and HTML code used to program the rest of the website. Plaintiff's argument thus suggests that every website on the internet—by recording and storing information, even temporarily, to facilitate a user's access to a website—uses an "intercepting device" and potentially violates the Wiretap Act. Websites that use data analytics tools are different only in that they purportedly embed an "intercepting device" within an "intercepting device." Rather than adopt that absurd result, the Court should hold that computer code is not an "intercepting device."

2. Even if Computer Code Were a Device, the Ordinary Course of Business Exception Would Apply.

The Wiretap Act exempts from the term "intercepting device" "any telephone or telegraph instrument, equipment, facility, or a component thereof . . . being used by a communications common carrier in the ordinary course of its business." G.L. c. 272, § 99(B)(3). The Superior Court held that this exception does not apply to website analytics tools because it requires that the "intercepting device at issue [] consist of or include 'telephone or telegraph' equipment, instruments, etc." R:A:VII:71–72 (quoting G.L. c. 272, § 99(B)(3)). But if "intercepting device" is interpreted broadly enough to cover website code, the exemption should be given a similarly broad construction.

The decision in *Dillon v. Massachusetts Bay Transportation Authority*, 49 Mass. App. Ct. 309 (2000), which this Court has cited approvingly, *see Moody v. Commonwealth*, 466 Mass. 197, 207 (2013), supports broad application of the exception. The *Dillon* court held that "a deviation" from the literal wording of the Wiretap Act was justified where "unusual circumstances" are presented and that the ordinary-course exception should be read "so as to preserve it in its intrinsic intended scope and maintain its viability in the broad run of cases." 49 Mass. App. Ct. at 315–16 (concluding that literal readings of the terms "communications common carrier" and "telephone equipment" do not limit applicability of the exception).

This case presents a novel theory and unusual circumstances that similarly counsel against a literal interpretation of the ordinary-course exception. As in *Dillon*, "the [Plaintiff's] proposal would in effect destroy the exception" by considering website code an "intercepting device" while categorically excluding website code from the ordinary course of business exception. *Dillon*, 49 Mass. App. Ct. at 315. In order to "comport[] with the canons that interpretation should tend to preserve the substance of a statute rather than diminish it," and refrain from "overriding common sense" or "produc[ing] absurd or unreasonable results," the Court should treat the use of website analytics tools as within the statutory exclusion to the "intercepting device" definition. *Dillon*, 49 Mass. App. Ct. at 315–16. Holding otherwise would conflict with this Court's canons of interpretations, the legislative intent of the Wiretap Act, and common sense. While the best interpretation of the statute is the one given it in the 1960s, if this Court chooses to update the meaning of device to account for online activity, it must consistently update the meaning of the exception.

B. The Website Analytics Tools Did Not Collect "Communications."

The Wiretap Act prohibits the interception of "oral or wire communications." G.L. c. 272, § 99(Q). The statute does not define "communications," but based on the term's ordinary meaning, it refers only to an exchange of thoughts or ideas between people. It does not refer to a business's observations of how visitors use its website.

When the Wiretap Act was enacted, "communication" meant a conversation or exchange of ideas between people. *See, e.g.*, *Webster's Seventh New Collegiate Dictionary* 168 (1967) (defining "communication" as "a verbal or written message"); *New Webster's Encyclopedic Dictionary* 167 (1969) (defining "communication" as "information or intelligence imparted by word or writing; a document or message imparting information").

The history and purpose of the Wiretap Act confirm this interpretation. As this Court explained, the "Legislature was concerned principally with the investigative use of surveillance devices by law enforcement officials to eavesdrop surreptitiously on *conversations*." *Commonwealth v. Du*, 103 Mass. App. Ct. 469, 473–74 (2023) (quoting *Rainey*, 491 Mass. at 645) (emphasis added). "As reflected in its preamble, the wiretap statute was enacted to give due protection to the privacy of individuals by barring the secret use of electronic surveillance devices for *eavesdropping purposes*." *Dillon*, 49 Mass. App. Ct. at 310 (emphasis added).

Interpreting the Act "consistent with the statutory purpose," *Curtatone v. Barstool Sports, Inc.*, 487 Mass. 655, 659 (2021), this Court has held that the statute applies to exchanges that "capture or reveal the defendants' thoughts or knowledge about some fact or subject." *Commonwealth v. Gordon*, 422 Mass. 816, 833 (1996); *see also Commonwealth v. Rivera*, 445 Mass. 119, 127 n.10 (2005) (legislature was

"concerned with the protection of private 'conversations'"—in other words, the "exchange of sentiments, observations, opinions, ideas.").

This Court has repeatedly refused to apply the Wiretap Act when a conversation was not involved. *See, e.g.*, *Gordon*, 422 Mass. at 832–33 (Act inapplicable to "audiotaping of booking procedures" because these "purely administrative bookings steps" "did not capture or reveal the defendants' thoughts or knowledge about some fact or subject"); *Rivera*, 445 Mass. at 127 n.10 (Act inapplicable where "defendant cannot reasonably claim that his recorded threats and obscenities were a 'conversation'"). For similar reasons, the Massachusetts Wiretap Act does not prohibit "recording purely visual images," *Commonwealth v. Rock*, 83 Mass. App. Ct. 1134 (2013), and data from GPS devices, *Commonwealth v. Connolly*, 454 Mass. 808, 825 (2009). *See also Commonwealth v. Wright*, 61 Mass. App. Ct. 790, 791 n.1 (2004) ("There is no express statutory prohibition against visual, as contrasted with sound, recordings."). Just as the Wiretap Act does not extend to video surveillance in a store, it also does not extend to online browsing. *See, e.g.*, *Cook*, 2023 WL 5529772, at *5; *see also supra* pp. 10–11.

This Court's decision in *Commonwealth v. Moody*, 466 Mass. 196 (2013), further demonstrates this point. There, the Court held that the Wiretap Act applied to cellular text messages, because "a text message is a *communication* transmitted

over a cellular network that travels in part by wire or cable or other like connection within a switching station." *Id.* at 208 (emphasis added).

Unlike in *Moody*, Plaintiff did not allege any "communication" that the website analytics tools allegedly captured. Website users do not participate in "conversations" with the website (or with the analytics tools) when they scroll through a site and click on links, because those movements do not "exchange . . . sentiments, observations, opinions, [or] ideas." *Rivera*, 445 Mass. at 127 n.10. Instead, those tools observe and record the users' movements and actions while on the website.

C. The Court Should Reject Plaintiff's Attempt to Expand the Wiretap Act to Prohibit the Use of New and Beneficial Internet Technologies.

These cases are part of a broader effort to rewrite state wiretap laws to prohibit the use of industry-standard internet tools. In hundreds of cases filed in courts across the country, plaintiffs have alleged similar violations of state wiretap laws based on the defendants' use of data analytics tools. *See* pp. 3, 15 *supra*. Because tools like Google Analytics and Meta Pixel are used by tens of millions of businesses, *id.* at 11, there is no shortage of potential defendants in these suits. The defendants here may both be hospitals, but other plaintiffs have brought suits against defendants in many other industries, including restaurants and retailers. The ubiquity of the

challenged data analytics tools means that Plaintiff's theory threatens the practices of businesses in every sector of the economy.

For the reasons discussed above, Plaintiff's claims are foreclosed by the text of the Wiretap Act. Moreover, as Defendants explain in their brief, any ambiguity in that text should be resolved in favor of interpreting the statute narrowly given that it is a criminal statute. *See* Defendants-Appellants' Am. Opening Br. at 20–26. But the Court should reject Plaintiff's broad reading of the statute for an additional reason: The legislature enacted the Wiretap Act in the 1960s to address a specific issue of concern at that time—the use of "bugs" to intercept phone calls and similar person-to-person communications. That legislature could not have contemplated the technology at issue here—the use of data analytics tools to improve the user experience on internet websites.

Rather than rewriting the statute to cover this new technology, the Court should interpret the statute as written and leave the weighing of the costs and benefits of modern internet technology to the legislature. *See, e.g., Commonwealth v. Cartagena*, 71 Mass. App. Ct. 907, 909 (2008) ("Any expansion of the statutory mandate is within the province of the Legislature, not an appellate court." (citation omitted)).

CONCLUSION

For the foregoing reasons, this Court should reverse.

March 13, 2024

Respectfully submitted,

By: */s/ Michael M. Maya*

Emily Johnson Henn (*pro hac vice pending*)
COVINGTON & BURLING LLP
3000 El Camino Real
5 Palo Alto Square, 10th Floor
Palo Alto, CA 94306
Telephone: (650) 632-4700
ehenn@cov.com

Geoffrey Hobart, BBO No. 547499
COVINGTON & BURLING LLP
One International Place
Suite 1020
Boston, MA 02110
Telephone: (617) 603-8800
ghobart@cov.com

Mark W. Mosier (*pro hac vice pending*)
Michael M. Maya, BBO No. 672847
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW
Washington, DC 20001
Telephone: (202) 662-6000
mmosier@cov.com
mmaya@cov.com

Counsel for the Chamber of Commerce of the United States of America

CERTIFICATE OF COMPLIANCE

I certify that this brief complies with the Massachusetts Rules of Appellate Procedure that pertain to the filing of briefs, including, but not limited to those specified in Rule 16(k), 17, and 20. It complies with the type-volume limitation of Rule 20(a)(2)(C) as it contains 4,867 non-excluded words. It complies with the type-style requirements of Rule 20 because it has been prepared in proportionally spaced typeface using Microsoft Word 2016 in 14-point Times New Roman font.

/s/ Michael M. Maya

CERTIFICATE OF SERVICE

Pursuant to Massachusetts Rule of Appellate Procedure 13(e), I certify that on March 13, 2024, I made service of this brief *amicus curiae* in *Vita v. New England Baptist Hospital*, No. SJC-13542, before the Supreme Judicial Court, upon the attorneys of record for each party listed below via the Electronic Filing System.

For Plaintiff-Appellee:

Edward F. Haber
Michelle H. Blauner
Patrick J. Vallely
SHAPIRO HABER & URMY LLP
One Boston Place, #2600
Boston, MA 02108
ehaber@shulaw.com
mblauner@shulaw.com
pvallely@shulaw.com

For Defendants-Appellants:

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

/s/ Michael M. Maya

Michael M. Maya, BBO No. 672847
COVINGTON & BURLING LLP
One CityCenter
850 Tenth Street, NW

Washington, DC 20001
Telephone: (202) 662-6000
mmaya@cov.com

.