SJC-13542

KATHLEEN VITA[1] vs. NEW ENGLAND BAPTIST HOSPITAL (and a consolidated case[2]).

Suffolk. April 3, 2024. - October 24, 2024.

Present: Budd, C.J., Gaziano, Kafker, Wendlandt, Georges, & Dewar, JJ.

Electronic Surveillance. Hospital. Internet. Statute, Construction. Practice, Civil, Standing, Motion to dismiss. Words, "Communication," "Interception."

Civil actions commenced in the Superior Court Department on February 24 and April 7, 2023.

Motions to dismiss were heard by Hélène Kazanjian, J., and the cases were reported by her to the Appeals Court.

The Supreme Judicial Court granted an application for direct appellate review.

David Quinn Gacioch (Annabel Rodriguez also present) for the defendants.

Patrick J. Vallely (Edward F. Haber & Michelle H. Blauner also present) for the plaintiff.

---

[1] Individually and on behalf of all others similarly situated.

[2] Kathleen Vita vs. Beth Israel Deaconess Medical Center, Inc.

The following submitted briefs for amici curiae:

J. Tucker Merrigan, Victoria Santoro Mair, Ryan M. Hawkins, Ryan P. McManus, Dylan S. O'Sullivan, & Justin Kenney for John Doe & others.

John Pagliaro & Daniel B. Winslow for New England Legal Foundation & another.

Michael J. Tuteur, Lawrence W. Vernaglia, & Morgan McDonald for Massachusetts Health and Hospital Association, Inc., & another.

John Roddy & Elizabeth Ryan for National Consumer Law Center, Inc., & another.

Michael Vatis, of New York, & Michael J. Mozes for National Retail Federation & another.

Emily Johnson Henn, of California, Mark W. Mosier, of the District of Columbia, Geoffrey Hobart, & Michael W. Maya for Chamber of Commerce of the United States of America.

Elka T. Sachs, Ian D. Roffman, Seth P. Berman, Natalie M. Cappellazzo, & Natalia Peña for Greater Boston Chamber of Commerce & another.

Robert Kingsley Smith, Neal Quenzer, & Tobi Henzer for Pioneer Public Interest Law Center.

KAFKER, J. The plaintiff, Kathleen Vita, alleges that the defendants, New England Baptist Hospital (NEBH) and Beth Israel Deaconess Medical Center, Inc. (BIDMC) (collectively, hospitals), violated G. L. c. 272, § 99 (wiretap act or act), by collecting and transmitting her browsing activities on the hospitals' websites. In particular, her complaints against the defendants allege that she accessed and reviewed information available to the public on the hospitals' websites regarding doctors (including their credentials and backgrounds) and medical symptoms, conditions, and procedures, and that these interactions with the websites fall within the meaning of "wire communication[s]" protected by the wiretap act. Where the

hospitals allegedly shared information regarding Vita's browsing with third parties for advertising purposes without her consent, Vita alleges the hospitals violated the wiretap act by "intercept[ing]" her communications. Vita does not allege that private patient records or messages to nurses, doctors, or other healthcare providers were intercepted.

Based on our review of the text of the wiretap act and its legislative history, we cannot conclude with any confidence that the Legislature intended "communication" to extend so broadly as to criminalize the interception of web browsing and other such interactions. When the statute was enacted, wiretaps involved the interception of person-to-person conversations and messages using hidden electronic surveillance devices placed in people's homes or businesses or tapping their telephone lines. See Commonwealth v. Rainey, 491 Mass. 632, 645 (2023) (Legislature's chief concern in enacting wiretap act was "electronic eavesdropping" and wiretapping [citation omitted]). The Legislature crafted the statute to prohibit new and evolving technological means of secret electronic eavesdropping on such person-to-person conversations or messaging, whether they be face-to-face conversations, calls on a landline telephone, cell phone calls, text messages, Internet chats with other people, e-mail messages, or other interpersonal conversations or messaging utilizing future technology. However, Vita's

allegations do not claim the interception of person-to-person conversations or messaging of the kind clearly within the wiretap act's ambit. The interactions here are not with another person but with a website. Nor are they personal conversations or messages being intercepted, but rather the tracking of a website user's browsing of, and interaction with, information published on a website.

As explained infra, nothing in the text of the statute makes unambiguously clear that the Legislature intended to reach so far as to criminalize the secret recording of such web browsing activities. The statute's text does not define "communication"; its text contains numerous references to communications that are person-to-person; and dictionary definitions do not provide a firm answer either way. The legislative history is focused on the secret interception of person-to-person conversations and messaging, particularly private ones. While the Legislature plainly intended the wiretap act to prohibit future technological means of such interceptions, it is not at all clear that the Legislature intended the statute's prohibition on intercepting "communications" to include, as supposed "communications," the web browsing alleged here.

Because the meaning of "communication" in this context is ambiguous, we must therefore apply the rule of lenity. When "we

find that the statute is ambiguous or are unable to ascertain the intent of the Legislature, the defendant is entitled to the benefit of any rational doubt" (citation omitted). Commonwealth v. Montarvo, 486 Mass. 535, 542 (2020).

If the Legislature intends for the wiretap act's criminal and civil penalties to prohibit the tracking of a person's browsing of, and interaction with, published information on websites, it must say so expressly. Other States and the Federal government have attempted to update their wiretap laws in response to technological change and done so in a variety of ways.

Make no mistake, the hospitals' alleged conduct here raises serious concerns, and may indeed violate various other statutes and give rise to common-law causes of action more specifically directed at the improper handling of confidential information, particularly confidential medical information. And we do not in any way minimize the serious threat to privacy presented by the proliferation of third-party tracking of an individual's website browsing activity for advertising purposes. These concerns, however, should be addressed to the Legislature.

Because we conclude that the statute is ambiguous and the rule of lenity should apply, we reverse the Superior Court judge's denial of the hospitals' motions to dismiss.[3]

1. Background. a. Facts alleged. "We summarize the factual allegations set forth in the complaint[s] and in the undisputed documents incorporated by reference in the complaint[s,] . . . accepting as true all well-pleaded facts alleged" (quotation omitted). Six Bros., Inc. v. Brookline, 493 Mass. 616, 618 (2024), quoting Osborne-Trussell v. Children's Hosp. Corp., 488 Mass. 248, 250, 253 (2021).

i. Hospital websites. BIDMC and NEBH operate hospitals in the Commonwealth, providing care to patients in Boston and the surrounding communities. The hospitals maintain websites, which provide general information about the hospitals and other medical information to patients and the public. Although the websites also contain separate patient portals containing patients' personal medical information, Vita does not allege

[3] We acknowledge the briefs of amici curiae Chamber of Commerce of the United States of America; Greater Boston Chamber of Commerce and Massachusetts Nonprofit Network; Doe plaintiffs in other pending civil actions; Massachusetts Health and Hospital Association, Inc., and Massachusetts Medical Society; National Retail Federation and Retailers Association of Massachusetts; National Consumer Law Center, Inc., and Electronic Privacy Information Center, Inc.; New England Legal Foundation and Associated Industries of Massachusetts; and Pioneer Public Interest Law Center.

that the information contained on such patient portals was intercepted or transmitted to others.

Each hospital's website provided the following: general information about the respective hospital; information about healthcare services available at each provider, addressing specific practice areas and health conditions; a "Find a Doctor" function to search for physicians by specialty and location; a portal for patients to access and to pay their medical bills online; a portal for patients to access their individualized medical information; and a feature for users to enter search terms to query information collected on the website. BIDMC's website additionally provided medical information about specific health conditions, including information on symptoms, causes, diagnoses, and treatments, and it also allowed patients to schedule appointments through an online portal.

ii. Vita's browsing activities. While the complaints make numerous allegations regarding users of the hospitals' websites generally, which we describe below, Vita alleges that she herself regularly used the websites to (1) obtain information about doctors (including their credentials and backgrounds); (2) search for information on particular symptoms, conditions, and medical procedures, both for herself and her husband; and (3) obtain and review her husband's medical records through the website's patient portal. She does not, however, allege that

her husband's medical records or the contents of his patient portal were in any way collected, intercepted, and transferred to third parties; that any messages between her or her husband or other users and health care professionals were intercepted or transmitted to others; or that she used the hospitals' websites to schedule appointments.

iii. Data that the hospitals allegedly collected.[4] Although not specific to Vita's own use of the hospitals' websites, the complaints also allege that the hospitals tracked the following information regarding users visiting the hospitals' websites: (1) the uniform resource locator (URL)[5] of the webpages visited; (2) the titles of those webpages; (3) data about a user's web browser and device configurations (e.g., screen resolution, device information, and browser settings); (4) the unique identifiers used by third-party software providers to track individuals across the website; and (5) a

---

[4] While the dissent refers broadly to interception of "private healthcare information," post at , there is no allegation that information contained within the private patient portals was accessed or shared.

[5] As described in the complaint against BIDMC:

> "A 'URL' is another form of an address specifically for websites . . . that a web browser can translate into an [Internet protocol (IP)] address to load the website. . . . Numerous URLs also point to specific pages on that website; often, a URL will contain information about the particular webpage itself."

user's Internet protocol (IP)[6] address. According to the complaints, this information permitted third-party software providers to create "browser fingerprints," which were capable of associating a particular individual with a unique combination of web browser settings.

Vita also alleges that certain information about a user's activities on the hospitals' websites was collected. This information included the following: (1) how, when, and where a user scrolled and clicked through different parts of a webpage;[7] (2) whether a user navigated to a webpage containing a form for new patients requesting appointments, as well as the department the user selected, and whether the user submitted the form, although not the information the user entered into the form (with the exception of the department selection);[8] (3) the contents of any search a user made on the websites; (4) the

---

[6] Vita's complaints explain that "[a]n 'IP address' is a unique combination of . . . numbers . . . that serves as a particular device's address on the [I]nternet."

[7] This was allegedly collected only on BIDMC's website, which implemented an optional feature offered by Google Analytics.

[8] While Vita alleges that users could book appointments and reserve spots in line to be seen by an urgent care physician, nothing indicates that users could engage in substantive written conversations or draft particularized messages to health care providers using the forms. Nor does Vita allege that she herself used the form to request appointments.

filtering criteria selected by a user on the "Find a Doctor" webpage, including specialty, location, gender, and language; (5) whether the user "reserved a spot" in line at the hospitals' urgent care; (6) whether the user navigated to the webpage for paying medical bills; (7) whether the user navigated to the patient portal where the user could access medical records and other personal medical information, although not the contents of records or communications within that portal; and (8) whether, when navigating to the patient portal, the user clicked the "login" button for existing patients or the "sign up now" button for patients seeking to create new accounts.[9]

iv. Third-party tracking software and the sharing of such information for marketing purposes. Vita alleges that the websites contained tracking software, developed by third parties, that allowed the hospitals and third parties to monitor the use of the hospitals' websites. These third parties included Facebook and Google, each offering similar software, "Meta Pixel" and "Google Analytics," which allowed hospitals to track user activity on their websites. The software simultaneously collected and transmitted to the third-party software providers information about the websites' users and the users' interactions with the websites. The third-party software

[9] The software on NEBH's site also would transmit the name of the user's doctor.

providers, in turn, marketed the data to merchants and delivered targeted digital advertisements tailored to individual users. Vita's complaints allege that this widespread targeted marketing activity is highly significant economically. According to the complaint, "Google derives a substantial portion of its revenues through individually targeted advertising," and "Facebook derives most of its revenues from selling targeted advertising to users of its platforms, including Facebook and Instagram."[10]

v. The hospitals' disclosures. The hospitals included a pop-up message on their websites disclosing, "We use cookies and other tools to enhance your experience on our website and to analyze our web traffic." The pop-up messages linked to privacy policies summarized below.[11] Both hospitals had in place nearly identical privacy policies. The policies (inaccurately and misleadingly, according to Vita) reassured users that

> "[the hospital] is committed to protecting your privacy. The [hospital's] website allows you to visit most areas without identifying yourself or providing personal

[10] As explained in the briefing by both parties and the amicus submissions, such tracking is commonly employed. See Amended Opening Brief for Defendants-Appellants, at 24-25; Brief for National Retail Federation and Retailers Association of Massachusetts, as Amici Curiae, at 3 ("The technologies at issue in this case are found on all manner of websites[] and play a fundamental role in the modern digital economy . . .").

[11] The complaints do not allege whether Vita viewed the pop-up messages when she accessed the webpages or whether she reviewed the privacy policies. The complaints also do not allege how or when the pop-up messages first appeared to a user navigating the websites.

> information. For those areas where you elect to provide identifiable information, we assure you that we make every effort to protect your privacy."

The hospitals also disclosed that they "routinely gather[ed] 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.," to "improve site content and overall usage." However, the hospitals represented that such data "is collected on an aggregate, anonymous basis, which means no personally identifiable information is associated with the data." The hospitals further claimed that "[t]his information is not shared with other organizations" and that "[e]xcept for authorized law enforcement investigations or other facially valid legal processes, we will not share any information we receive with any outside parties."

The privacy policies also disclosed (albeit again allegedly incompletely and misleadingly) some third-party data tracking or sharing. The hospitals stated that they and their "Third Party Service Provider[s]" collected and saved "the default information customarily logged by worldwide web server software," which included "date and time, originating IP address and domain name[12] . . . , object requested, and completion

---

[12] A domain name, as defined in the privacy policies, is "the unique address assigned to your Internet service provider's computer that connects to the Internet."

status of the request." They further disclosed that this information "may be kept for an indefinite amount of time, [and] used at any time and in any way necessary to prevent security breaches and to ensure the integrity of the data on our servers."

b. Prior proceedings. Vita filed separate complaints -- one against BIDMC and one against NEBH -- each alleging, on Vita's behalf and purportedly on behalf of a class of similarly situated persons,[13] that the hospital violated the wiretap act by aiding the third-party software providers to intercept communications. Each hospital separately filed a motion to dismiss pursuant to Mass. R. Civ. P. 12 (b) (6), 365 Mass. 754 (1974). A Superior Court judge denied both motions in separate opinions; she reported her decisions to the Appeals Court pursuant to Mass. R. Civ. P. 64 (a), as amended, 423 Mass. 1403 (1996). Subsequently, we allowed the hospitals' consolidated request for direct appellate review.

2. Discussion. a. Standard of review. "We review the denial of a motion to dismiss under Mass. R. Civ. P. 12 (b) (6)

[13] No class had been certified by the time these cases reached this court. There has also been no other plaintiff identified. Based on our decision today, we need not address whether the prerequisites of class certification, including whether Vita is an appropriate class representative, may be satisfied here. See Mass. R. Civ. P. 23, as amended, 471 Mass. 1491 (2015).

. . . de novo." Marsh v. Massachusetts Coastal R.R., 492 Mass. 641, 645 (2023), cert. denied, 144 S. Ct. 2519 (2024), quoting Dunn v. Genzyme Corp., 486 Mass. 713, 717 (2021). "In doing so, we accept 'as true all well-pleaded facts alleged in the complaint, drawing all reasonable inferences therefrom in the plaintiff's favor, and determining whether the allegations plausibly suggest that the plaintiff is entitled to relief.'" Marsh, supra at 645-646, quoting Lanier v. President & Fellows of Harvard College, 490 Mass. 37, 43 (2022).[14] See Iannacchino v. Ford Motor Co., 451 Mass. 623, 636 (2008) ("Factual allegations must be enough to raise a right to relief above the speculative level . . ." [citation omitted]).

b. Standing. We first address the hospitals' argument that Vita has not alleged an actual injury arising from the hospitals allegedly aiding third-party software providers to

[14] The dissent claims we apply "a heightened pleading standard, or a premature analysis of whether Vita is an appropriate class representative." Post at . We do not. As we note infra, we need not and do not decide whether Vita is an appropriate class representative, although we are cognizant that she is the only class representative identified and her personal claims are quite limited. Although we do not ignore Vita's allegations as to what users in general did on the websites, we do not, as the dissent does, embellish those allegations or her own. See, e.g., notes 4, 8, supra; notes 21, 22, infra. As no class has been certified and Vita may not be an appropriate class representative, we also make clear, where we can, what she alleges she experienced and what unknown other members of a putative class may allege. If anyone is straining pleading standards, it is the dissent.

record secretly her interactions with the hospitals' websites; thus, they contend, Vita lacks standing to pursue a claim under the wiretap act. See Murchison v. Zoning Bd. of Appeals of Sherborn, 485 Mass. 209, 218 (2020) (where plaintiffs "lack standing . . . we order[] dismissal of the appeal without reaching the merits").

A plaintiff bears the burden of establishing standing to bring a cause of action; more specifically, at this stage, she must plead facts sufficient to "demonstrate a nonspeculative particular and personal harm" resulting from the challenged action. Murchison, 485 Mass. at 212. See Animal Legal Defense Fund, Inc. v. Fisheries & Wildlife Bd., 416 Mass. 635, 638 (1993) ("only persons who have themselves suffered, or who are in danger of suffering, legal harm can compel the courts to assume the difficult and delicate duty of passing upon the validity of the acts of [another] branch of government" [citation omitted]). "A party has standing when [she] can allege an injury within the area of concern of the statute or regulatory scheme under which the injurious action has occurred." Penal Insts. Comm'r for Suffolk County. V. Commissioner of Correction, 382 Mass. 527, 532 (1981), quoting Massachusetts Ass'n of Indep. Ins. Agents & Brokers v. Commissioner of Ins., 373 Mass. 290, 293 (1977).

Thus, to determine whether a plaintiff has standing, we look to the statute itself to determine whether the Legislature intended to confer standing to a person in the plaintiff's position. See, e.g., Massachusetts State Auto. Dealers Ass'n v. Tesla Motors MA, Inc., 469 Mass. 675, 683 (2014). Relevant here, the wiretap act provides a private cause of action to "[a]ny 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."[15] G. L. c. 272, § 99 Q. The act further provides for statutory damages, regardless of whether the aggrieved person suffered any actual damages. Id.

Vita alleges that the hospitals violated the act by assisting third parties to record contemporaneously her interactions with the hospitals' websites without her consent or knowledge. In her case, those allegations are limited to searching for information related to doctors and symptoms on the websites. This alleged violation of the act falls "within the area of concern of the statute . . . under which the injurious

---

[15] The act defines an "aggrieved person" as "any individual who was a party to an intercepted wire or oral communication . . . or who would otherwise have standing to complain that his personal or property interest or privacy was invaded in the course of an interception." G. L. c. 272, § 99 B 6.

action has occurred." Penal Insts. Comm'r for Suffolk County, 382 Mass. at 532, quoting Massachusetts Ass'n of Indep. Ins. Agents & Brokers, 373 Mass. at 293. See Pine v. Rust, 404 Mass. 411, 414 (1989) (wiretap act "grants a civil remedy to any aggrieved person whose communications were intercepted, disclosed, or used, except as authorized by the statute"). Thus, Vita has established standing regarding these claims because she has alleged a particular, personalized, nonspeculative, injury arising from an alleged violation of the act.[16]

c. Statutory construction. As Vita has standing to pursue her personal allegations, we turn to the main issues in these cases, particularly the meaning of "communication" and "interception" under the act, which are questions of statutory interpretation.

---

[16] As discussed supra, the complaints outline various other claims presented on the behalf of currently unnamed members of the purported class. Because there are no other named plaintiffs in these cases, Vita's individual standing is particularly important. Cf. Gammella v. P.F. Chang's China Bistro, Inc., 482 Mass. 1, 20 (2019) (recognizing that whether plaintiff's claim was moot was "particularly important . . . because no other named plaintiff [had] yet been identified"). As we conclude that Vita has standing regarding her claims, however, we need not decide whether she would independently have standing to pursue other claims on behalf of the class. Contrast Weld v. Glaxo Wellcome Inc., 434 Mass. 81, 84 (2001) (class representative lacked standing where he had suffered no individual injury).

> "[A] statute must be interpreted according to the intent of the Legislature ascertained from all its words construed by the ordinary and approved usage of the language, considered in connection with the cause of its enactment, the mischief or imperfection to be remedied and the main object to be accomplished, to the end that the purpose of its framers may be effectuated" (citation omitted).

Harvard Crimson, Inc. v. President & Fellows of Harvard College, 445 Mass. 745, 749 (2006). We begin with a statute's plain language. See Matter of the Estate of Mason, 493 Mass. 148, 151-152 (2023). We do not "interpret words in a statute in isolation"; rather, we "must look to the statutory scheme as a whole so as to produce an internal consistency within the statute." Outfront Media LLC v. Assessors of Boston, 493 Mass. 811, 818 (2024), quoting Plymouth Retirement Bd. v. Contributory Retirement Appeal Bd., 483 Mass. 600, 605 (2019).

"Ordinarily, where the language of a statute is plain and unambiguous, it is conclusive as to legislative intent." Six Bros., Inc., 493 Mass. at 622, quoting Sharris v. Commonwealth, 480 Mass. 586, 594 (2018). But "[w]here the statutory language is not conclusive, we may 'turn to extrinsic sources, including the legislative history and other statutes, for assistance in our interpretation.'" HSBC Bank USA, N.A. v. Morris, 490 Mass. 322, 332-333 (2022), quoting Chandler v. County Comm'rs of Nantucket County, 437 Mass. 430, 435 (2002).

i. Statutory background. The wiretap act makes it a crime to "willfully commit[] an interception, attempt[] to commit an

interception, or procure[] any other person to commit an interception or to attempt to commit an interception of any wire or oral communication." G. L. c. 272, § 99 C 1. "Wire communication" is defined 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." G. L. c. 272, § 99 B 1. An "oral communication" is "speech, except such speech as is transmitted over the public air waves by radio or other similar device." G. L. c. 272, § 99 B 2. "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." G. L. c. 272, § 99 B 4.

The statute provides for both criminal penalties and a civil remedy for wiretap act violations. Willful interceptions of oral or wire communications are punishable by a fine of up to $10,000, imprisonment for up to five years, or a combination of fines and imprisonment.[17] G. L. c. 272, § 99 C 1. The act also

[17] The same punishments apply to anyone who "attempts to commit an interception, or procures any other person to commit an interception or to attempt to commit an interception." G. L. c. 272, § 99 C 1.

criminalizes the possession of an intercepting device or permitting another person to use such a device, which is a misdemeanor punishable by imprisonment of up to two years, a fine of $5,000, or both. G. L. c. 272, § 99 C 5. Willful disclosure or use of the contents of any wire or oral communication, knowing that the information was obtained through interception is also a misdemeanor with the same punishment. G. L. c. 272, § 99 C 3. The statute also provides a civil remedy for any "aggrieved person whose oral or wire communications were intercepted, disclosed or used except as permitted or authorized by [statute]." G. L. c. 272, § 99 Q. "[A]n interception need not rise to the level of criminal conduct covered by the penal provisions of the law" to support a civil claim; in particular, a civil claim does not require that the conduct be willful. Pine, 404 Mass. at 414. The act provides for "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," as well as punitive damages. G. L. c. 272, § 99 Q 1-2. A plaintiff is also entitled to attorney's fees and other litigation costs. G. L. c. 272, § 99 Q 3.

ii. Communication. Vita contends that the meaning of "communication" is broad enough to encompass all her alleged interactions with the hospitals' websites. We conclude that the

statutory term "communication" is ambiguous as applied to the web browsing activities allegedly intercepted. Neither the plain text of the statute nor dictionary definitions make clear whether such activity amounts to "communication," and the legislative history is concerned with a different type of surveillance. Thus, the rule of lenity must apply, thereby entitling the defendants to "the benefit of any rational doubt" in the construction of the statute (citation omitted). Montarvo, 486 Mass. at 542.

General Laws c. 272, § 99, does not define the word "communication," but rather the means or method of "communication" -- i.e., wire or oral.[18] The statute does include, however, a number of examples of communications that shed at least some light on the Legislature's intended meaning. For example, one of the requirements for a warrant under the

[18] The dissent emphasizes the word "any" that accompanies the definition of "wire communication," asserting that the use of "any" to modify "communication" evinces a clear legislative intent to "provide sweeping protection for communications of whatever kind" (quotation and citation omitted). Post at . See G. L. c. 272, § 99 B 1. The problem with this analysis, as explained supra, is that the term "wire communication" does not itself define the meaning of "communication," but rather the means of communication. We need to look to a source beyond the definition of "wire communication" to understand what "communication" means. Indeed, the dissent does this by turning to dictionaries for its interpretation of "communication." We address the problems with the dissent's dictionary analysis infra.

wiretap act is "[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" (emphasis added). G. L. c. 272, § 99 F 2 e. The statute also repeatedly references telephones and telegraphs, carving out permissible activities in relation thereto. See G. L. c. 272, § 99 B 3, D 1, F 2, I 3, J 1, L 1 (telephone); G. L. c. 272, § 99 B 3, F 2, I 3, J 1, L 1 (telegraph).[19] The statute's text thus makes plain the Legislature's intent to address at least conversations in person or over the telephone or person-to-person messages communicated through the use of wire or cables. Accordingly, it does seem clear that the plain meaning of "communication" includes messages and conversations[20] between people through the use of

[19] According to the dissent, these references to "telephone" and "telegraph" are just examples of the Legislature explicitly limiting a provision of the act to a particular type of communication. The act requires that warrant applications include a statement "[t]hat the oral or wire communications of the particularly described person . . . will occur . . . over particularly described telephone or telegraph lines" (emphasis added). G. L. c. 272, § 99 F 2 c. Similarly, a warrant must include "[a] particular description of the person and the place, premises or telephone or telegraph line upon which the interception may be conducted" (emphasis added). G. L. c. 272, § 99 I 3. It is not clear why the Legislature would want to limit the warrant requirements to telegraph or telephone lines as opposed to other types of wired communications.

[20] A conversation is an "oral exchange of sentiments, observations, opinions, or ideas," and includes a similar

wire or cable, including by means of e-mail, text message, chat, instant message, or the equivalent. Indeed, conversations and messages between people accord with our common understanding of communications. Private conversations in person or over the telephone or private person-to-person messages communicated through the use of wire or cables are the core type of communication the wiretap law was designed to address. E-mail messages and text messages also plainly involve person-to-person messaging over a wire or cable, so those too fall within the plain meaning. Similarly, online chats and instant messaging, where actual people communicate with each other, are plainly covered as well, as they involve person-to-person messaging over a wire or cable.

Notably, however, Vita's complaints do not allege communications between people in this commonsense way. The complaints repeatedly characterize the intercepted communications as being between Vita and each hospital's website, not between Vita and hospital personnel, understandably, given that the allegedly intercepted communications consist of what would commonly be called web

---

exchange conducted by, for example, e-mail. Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/conversation [https://perma.cc/EL4B-75K2].

browsing by Vita.[21] It is far less clear based on the plain text of the statute that the term "communication" extends to all interactions between a user and a website. When a user browses a public website, and accesses databases and other information readily available to anyone on the Internet, the user is not speaking or messaging with another person but rather interacting with the website; the user is also not engaged in personal conversation or messaging but rather browsing and interacting with the published information on the website.[22]

---

[21] The dissent claims we rely on Vita's allegations that she communicated with the hospitals' websites but ignore places in the complaints where she characterizes the communications as between users and the hospitals. But there is nothing in the allegations to suggest that anything other than interactions with the website are at issue here. When the complaints reference communications with the hospitals, they are only referencing communications with the hospitals' websites. As discussed supra, there is a significant difference between communicating with a person and communicating with a website, a difference the dissent fails to grasp. According to the dissent, there is no meaningful difference between speaking to a doctor about one's specific illness and searching for, and then reading, pre-generated content on a webpage discussing an illness in general. There is a difference in kind and not degree between the two as we explain throughout the opinion. One is interpersonal, the other is not.

[22] The dissent says we "misapprehend[] the hospitals' websites as repositories for 'published,' 'pre-generated' medical data," and contends that the websites were in fact "confidential dynamic forums on which [the hospitals] communicated 'interactive[ly]' with patients about the patients' 'personal' medical needs." Post at . We disagree with the dissent's characterization. Nothing in the complaints indicates that the hospitals provided specific, tailored responses in real time to users' inquiries. As alleged here, the content was no

While we often turn to dictionaries to aid in understanding the plain meaning of undefined statutory terms, here, dictionaries do not provide a ready answer to the question whether web browsing activities of the kind Vita alleges she engaged in amount to "communication" with the website on which one is browsing or with the website's owner or author.[23] Most

---

more dynamic than that contained on any other website that provides written content that is periodically updated. Nor do the complaints describe hospital websites that are more interactive than most institutional webpages that provide general information. Users had the ability to navigate and find information relevant to themselves and to schedule appointments, but nothing in the complaints indicates that, at least where third-party tracking was active on the websites, users could engage in one-on-one interactions with specific medical providers.

[23] The dissent claims we disregard the dictionary definitions of "communication." We do not. "Dictionaries can be useful in interpreting statutes, but judges . . . must take care not to 'overread' what dictionaries tell us" (citation omitted). Suesz v. Med-1 Solutions, LLC, 757 F.3d 636, 643-644 (7th Cir.), cert. denied, 574 U.S. 1047 (2014). "Although . . . dictionaries can be helpful -- especially when dealing with a specialized term, or a term of art, or a word's usage at the time of the law's enactment -- more often than not, the interpretive challenge comes from the ambiguity of the word as situated in a sentence. In that situation, dictionaries can hardly be definitive." R.A. Katzmann, Judging Statutes 43 (2014). Here, the dictionary definitions are too varied and "too vague to provide meaningful guidance." Suesz, supra at 643. In everyday language and in other legal contexts, "communication" can ordinarily imply an interpersonal exchange, such as a conversation or exchange of messages. See, e.g., Clair v. Clair, 464 Mass. 205, 213 (2013) (determining whether testimony and documents sought were privileged attorney-client communications); Phelan v. May Dep't Stores Co., 443 Mass. 52, 56 (2004) ("communication" for defamation purposes defined as "conduct that brings an idea to the perception of others"

definitions of "communication" refer to an "interchange" or "exchange" of information, implicitly between people, but without expressly defining who or what need be on either end.[24] Some definitions, are even more explicit, referencing persons or individuals on both sides of a communication, thereby strongly suggesting that mere accessing of information published on a website may not qualify. See, e.g., Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/communication [https://perma.cc/7VX3-KSG7] (defining communication as "a process by which information is exchanged between individuals through a common system of symbols, signs, or behavior" [emphasis added]); Oxford English Dictionary Online (defining communication as "[i]nterpersonal contact, social interaction, association, intercourse"); Black's Law Dictionary

---

[citation omitted]); Emerson, 8 Ways You Can Improve Your Communication Skills, Harvard Division of Continuing Education (Aug. 30, 2021), https://professional.dce.harvard.edu/blog/8-ways-you-can-improve-your-communication-skills [https://perma.cc/P4RD-WN75] ("A leader's ability to communicate clearly and effectively with employees, within teams, and across the organization is one of the foundations of a successful business").

[24] See, e.g., American Heritage Dictionary of the English Language 269 (1970) ("The exchange of thoughts, messages, or the like, as by speech, signals, or writing"); Random House Dictionary of the English Language 298 (1967) ("the imparting or interchange of thoughts opinions, or information by speech, writing, or signs").

350 (12th ed. 2024) (defining communication as "the process of bringing an idea to another's perception" [emphasis added]).

In attempting to argue nonetheless that the term "communication" in the statute does unambiguously encompass web browsing, Vita relies on the preamble of the wiretap act. The clause Vita focuses on states that "the uncontrolled development and unrestricted use of modern electronic surveillance devices pose grave dangers to the privacy of all citizens of the [C]ommonwealth," and thus the "secret use of such devices by private individuals must be prohibited." G. L. c. 272, § 99 A. This clause doubtless does state the Legislature's intent to protect the Commonwealth's citizens from the threat to privacy posed by evolving modern methods of electronic surveillance.[25] And, as discussed, the term "communication" in the wiretap act doubtless does extend today to protecting person-to-person communications from Internet-based means of interception. However, notwithstanding the clause's plain statement of the Legislature's intent to protect citizens' privacy against new surveillance methods, the clause does not directly address the

[25] We also note that most of the preamble is directed at the dangers presented by organized crime and the need for its secret surveillance, albeit under tight controls. See G. L. c. 272, § 99 A ("[O]rganized crime constitute[s] a grave danger to the public welfare and safety. . . . [L]aw enforcement officials must be permitted to use modern methods of electronic surveillance, under strict judicial supervision, when investigating these organized criminal activities").

nature of the protected communications themselves and whether, as here, the act protects against interception of the act of browsing a website, rather than a person-to-person communication.

Ultimately, we cannot conclude that the wiretap act unambiguously prohibits and, indeed, criminalizes the interception of web browsing activity, because there appears to be a difference in kind and not degree between interactions on a website available to the public and private conversations in your house or on your telephone. In essence, we are not here dealing with just new means of communication, such as the difference between communicating with another person on a cell phone rather than a landline, or a text message rather than a telegraph message. See Commonwealth v. Moody, 466 Mass. 196, 198 (2013) (concluding wiretap act applies to interception of cell phone calls and text messages). Browsing and accessing the information published on a website is significantly different from having a conversation or sending a message to another person.[26] As explained previously, the user is not communicating with another person but instead interfacing with pre-generated information on a website. The user is also not engaging in a

[26] We note that oral communication expressly excludes speech "transmitted over the public air waves by radio or other similar device." G. L. c. 272, § 99 B 2.

conversation but accessing published information and databases.[27] Given these differences, we cannot conclude based on the relevant text of the statute that the Legislature unambiguously intended to criminalize activities that do not capture such person-to-person communications or messaging.

In sum, the text of the wiretap act is inconclusive at best as to whether website browsing is a "communication" protected by the act.[28]

iii. Legislative history. As the text of the statute does not resolve the ambiguity, "we may 'turn to extrinsic sources, including the legislative history . . . for assistance in our interpretation.'" HSBC Bank USA, N.A., 490 Mass. at 332-333.

---

[28] The dissent accuses us of confusing the act's protection of the "contents" of a communication with the "communication" itself. Post at . The wiretap act defines "contents" as "any information concerning the identity of the parties to such communication or the existence, contents, substance, purport, or meaning of that communication." G. L. c. 272, § 99 B 5. The problem is that "contents," while referencing "communication," does not define the term. Moreover, the definition refers to "parties to such communication." This only reinforces the ambiguity of the definition of communication, as "parties" seems to suggest the existence of at least two individuals (i.e., two parties to a telephone call or two parties to a text message thread). See Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/party [https://perma.cc/2K4N-XPPE] ("party" can be defined as "a particular individual" or "a person or group participating in an action or affair"). Accordingly, where the meaning of "communication" is ambiguous, we cannot say with any more confidence that the information described by the dissent (e.g., URLs, titles of webpages, hyperlinks, etc.) is "contents" of a communication also protected by the wiretap act.

When we do so here, we conclude that the Legislature was chiefly concerned about the secret recording or monitoring of person-to-person communications. There is nothing in that legislative history suggesting that the Legislature intended to extend the act, and its criminal penalties, beyond the interception of person-to-person conversations or messaging.

From the very beginning, the Legislature repeatedly referred to eavesdropping on private conversations and the use of covert electronic recording devices that could be placed in a home or business or used to tap a telephone. In 1964 the Legislature established a commission for the "investigation and study of the laws relative to eavesdropping and the use of any electronic recording device, or wireless tap or electronic tap" (emphasis added). Senate Bill No. 201 (1964). See Commonwealth v. Tavares, 459 Mass. 289, 294-295 (2011).

An interim committee report from April 1967 described various eavesdropping devices that were commercially available. See 1967 Senate Doc. No. 1198, at 3. These included the "parasite bug," a "subminiature transmitter less than half the size of a pack of cigarettes, which broadcasts both sides of a telephone conversation." Id. There was also the "room bug," capable of "transmit[ting] a very clear signal at least [seven] blocks in downtown Boston" and "pick[ing] up a whisper at [twenty] feet." Id. See Rainey, 491 Mass. at 645 ("In April

1967, the commission issued an interim report, which focused on various types of 'eavesdropping devices,' namely 'bug[s]'"). The future development of such eavesdropping devices was recognized to be particularly "frightening" and unpredictable. See 1967 Senate Doc. No. 1198, at 4. See also Commonwealth v. Hyde, 434 Mass. 594, 608 n.7 (2001) (Marshall, C.J., dissenting) ("The [April] 1967 Report makes clear that what concerned the Legislature were 'eavesdropping devices' ['bugs'] and other sophisticated inventions of then-recent origin . . ."). This report also noted the recent discovery that the New England Telephone and Telegraph Company intercepted "customer-to-customer calls and customer-to-company calls" in order to check "the performance of the company's equipment and employees." 1967 Senate Doc. No. 1198, at 4. See Commonwealth v. Ennis, 439 Mass. 64, 68 n.10 (2003) (noting that special commission's concern about secret electronic eavesdropping by private citizens was spurred by not only testimony about bugging devices but also revelation that telephone company "secretly record[ed] private telephone calls").

Later commission reports also repeatedly referred to the recording of or listening in on private conversations. See, e.g., 1967 Senate Doc. No. 1469, at 2 ("the availability of instruments for overhearing secretly private conversations is immense"); 1968 Senate Doc. No. 1132, at 9 (proposing revision

of wiretap act "to strictly prohibit electronic eavesdropping and wiretapping of other persons' conversations without permission"). Commissioners Elliot B. Cole and William P. Homans, Jr., concurred in the legislative recommendations, but wrote separately to emphasize the importance of the all-party consent requirement in the proposed law. 1968 Senate Doc. No. 1132, at 10. They voiced an overarching concern about the secret interception and recording of private conversations, quoting an academic who explained that "the individual expresses his personality in private conversations." Id. at 12. See Hyde, 434 Mass. at 608 n.6 (Marshall, C.J., dissenting) ("A concurring report filed by two members of the special commission, [Cole and Homans], makes abundantly clear that the 'prohibition of wiretapping and eavesdropping by the public' was to protect the privacy of citizens engaged in personal conversations").

This legislative history is therefore directed at the invasion of privacy and threat to free expression from secret surveillance of private conversations. See Commonwealth v. Rivera, 445 Mass. 119, 127 n.10 (2005) ("The report giving rise to the statute noted repeatedly that the commissioners were concerned with the protection of private 'conversations,' particularly by devices used to monitor telephone lines and by devices placed in private locations"). Electronic "bugs" that

could be covertly placed in a home or business or that could tap a telephone line to listen in on such conversations were also of particular concern, and the Legislature recognized that scientific developments here were especially frightening. See 1967 Senate Doc. No. 1198, at 4; Rivera, supra.

As the Internet did not exist, there was, of course, no discussion of whether the tracking and sharing of a user's browsing or other activity, via software and computer code, on public websites would be considered criminal. Indeed, there was no discussion whatsoever of computers or software in the legislative history. Nor was there any discussion of what might be considered historic analogies to website analytics and advertising, such as television[29] stations monitoring what shows or commercials viewers were watching or businesses or nonprofit organizations tracking brick-and-mortar or mail-order purchasing decisions or inquiries, or compiling customer lists, and sharing such information with other businesses or nonprofits without the customer's consent. Any such discussion in the legislative history might have provided some suggestion that the Legislature was prepared to extend the application of the act, and thus the meaning of "communication" and "interception," well beyond the

[29] As noted earlier, speech "transmitted over the public air waves by radio or other similar device" was expressly excluded. G. L. c. 272, § 99 B 2.

covert interception of private conversations and private messages. There is, however, nothing like that in the legislative history.

The legislative history's discussion of the monitoring of person-to-person business telephone calls is also informative, as the Legislature ultimately concluded that such monitoring of person-to-person calls was permissible, at least for telephone companies and banks, if done in the ordinary course of business.[30] In allowing such monitoring even of person-to-person calls, the Legislature took into account practical business realities as well as privacy concerns.

In sum, the legislative history is focused on the secret interception of person-to-person conversations and messaging, particularly private ones. The electronic surveillance devices, and the "frightening" future of such devices, with which the Legislature was concerned were covert recording devices that could be used to "bug" one's home or business or tap one's telephone line to listen in on such conversations. The

---

[30] The act allows "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." G. L. c. 272, § 99 D 1 a. It also allows "a financial institution to record telephone communications with its corporate or institutional trading partners in the ordinary course of its business." G. L. c. 272, § 99 D 1 f.

Legislature also recognized that ordinary business realities needed to be considered, allowing some monitoring of even private person-to-person conversations. While the legislative history thus evinces a focus on addressing the privacy threats posed by evolving surveillance methods, it does not provide a basis for concluding that the Legislature intended that the term "communication" would itself over time extend beyond person-to-person communications, such as to encompass a human's interactions with a website. The legislative history therefore provides no sound basis for concluding that the tracking of human-website interactions for website analytics and digital advertising purposes, via commonly employed technologies, is a "communication" under the wiretap act.

d. Case law. Our case law has never extended the meaning of "communication" beyond person-to-person interactions. Rather, our cases have always involved the interception of person-to-person conversations and messages. See, e.g., Commonwealth v. Morris, 492 Mass. 498, 501 (2023) (defendant's interview with police recorded); Rainey, 491 Mass. at 633 (video and audio of victim's report to police officer recorded by body-worn camera); Curtatone v. Barstool Sports, Inc., 487 Mass. 655, 657-658 (2021) (telephone conversation recorded by blogger); Moody, 466 Mass. at 198 (text messages intercepted); Tavares, 459 Mass. at 294 (informant recorded conversations with

defendant using concealed recording device). None involved a person browsing or otherwise interacting with a public website. Most of the cases involved the interception of private interpersonal conversations, which we have emphasized is the core statutory concern. See Rivera, 445 Mass. at 127 n.10. Indeed, a crucial fact in Rainey and Morris, two cases in which we found no statutory violation, was that the recording at issue "was not being used as an investigative tool to secretly eavesdrop on an otherwise private conversation" (emphasis added). Morris, supra at 506, quoting Rainey, supra at 643-644.

Moreover, we have previously rejected broad interpretations of the word "communication" that expand the scope of the wiretap act well beyond the secret recordings of private conversations the Legislature intended to prevent.[31] See Commonwealth v.

---

[31] The dissent declares that we commit an "analytical misstep" in looking to cases where we interpreted the wiretap act and did not find it ambiguous, but nonetheless rejected certain literal readings. Post at . We are unaware of any rule, nor does the dissent cite one, requiring that -- in determining whether a statute is ambiguous -- we only rely on cases where that same statute was declared ambiguous. Based on our citation of those same cases, the dissent further asserts that we must determine that "the Legislature would regard as absurd" the application of the wiretap act to the alleged website activities. Id. at . The dissent is incorrect. Where the statute's definition of communication clearly applies, we still consider whether its application is absurd. See Commonwealth v. Mansur, 484 Mass. 172, 175 (2020) (statute's language must be given its ordinary meaning if language is "clear and unambiguous"; however, "we do not adhere blindly to a literal reading of a statute if doing so would yield an 'absurd'

Gordon, 422 Mass. 816, 832-833 (1996) (rejecting "literal" reading of act "as making unlawful the audiotaping of booking procedures without the knowledge of the persons being booked, and as subjecting the responsible police officers to severe penalties therefor" in absence of more specific evidence of Legislature's intent to do so). See also Morris, 492 Mass. at 506 (recording of defendant's voluntary statements to police after receiving Miranda warnings did not violate wiretap act absent indication Legislature intended such result); Rainey, 491 Mass. at 643-644 (rejecting application of wiretap act to body-worn camera recording by police officer of victim's statement even while acknowledging wiretap act "could be construed literally as the defendant suggests"). These cases are inconsistent with Vita's characterization of a legislative intent to provide broad protections for all website activities, even where they do not involve person-to-person conversations or messaging.

The cases Vita relies upon do not resolve the wiretap act's ambiguity in this regard. In Moody, 466 Mass. at 198, we held that the wiretap act applied to text messages and calls sent and

---

or 'illogical' result" [citations omitted]). In the instant cases, however, as we have explained throughout this opinion, the term "communication" does not clearly apply here. Rather, it is ambiguous.

received with cell phones.[32] It is difficult to extrapolate much from Moody's holding that cell phone text messages and calls are "wire communications" under the act because those forms of communication are clearly person-to-person conversations and messaging; the case just involved updated technology to make such calls and send such messages.

The cases cited by Vita and the dissent interpreting the Federal wiretap act, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 211 (1968) (Title III), do not resolve the ambiguity presented by

---

[32] The dissent claims that we misread Moody, ignoring its conclusion that the "State act was as expansive as the amended Federal counterpart." Post at . According to the dissent, Moody stands for the proposition that our wiretap act covers all forms of communication covered by the Federal wiretap act, Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 211 (1968) (Title III), as amended, including all forms of electronic communication as that term is defined by Title III. Post at . The dissent is incorrect. Moody is, of course, a more nuanced decision. There, the court concluded only that the wiretap act, on "the several particulars challenged by the defendants, is not repugnant to the provisions of the Federal act and is accordingly not preempted" (emphasis added; citation omitted). Moody, 466 Mass. at 205. More particularly, the court concluded the "existing language of the Massachusetts wiretap statute is broad enough to protect all forms of cellular telephone calls that utilize wire, cable, or other like connections, even if the use of such connections is only in switching stations." Id. at 207. In this respect, the court found "the Massachusetts wiretap statute is as protective as the amended Federal wiretap statute." Id. To reach this conclusion, the court did not need to determine whether our State wiretap act protected every type of communication protected by the amended Title III, because the limited question before the court was whether cell phone calls and text messages were protected.

our State's statute. These cases do not engage in depth, if at all, with the meaning of "communication." See, e.g., In re Facebook, Inc. Internet Tracking Litigation, 956 F.3d 589, 607 (9th Cir. 2020), cert. denied sub nom. Facebook, Inc. v. Davis, 141 S. Ct. 1684 (2021) (characterizing "GET requests," in which website transmits user's URL information to third-party website, as communication without analyzing meaning of communication). Further, Title III was amended by the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986), to cover "electronic communication," defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system." 18 U.S.C. § 2510(12). That amendment was drafted almost twenty years after our wiretap act, during at least the dawn of the personal computer era. See Chayka, The Birth of the Personal Computer, The New Yorker (May 18, 2023), https://www.newyorker.com/culture/infinite-scroll/the-birth-of-the-personal-computer [https://perma.cc/S6N9-PLFK] (noting that among first "microcomputer kits," was Altair 8800, which debuted in 1975, followed shortly by first Apple computer in 1976, and Apple II in 1977, which is considered precursor to modern personal computers). It is also no surprise then that cases applying Title III do not struggle over the definition of

"communication," because the broad definition of "electronic communication" would appear to cover many website browsing activities. However, our wiretap act was never similarly amended to add a separate definition of "electronic communication." Moody, 466 Mass. at 207-208.[33]

Title III also differs importantly from our wiretap act in providing a one-party consent exception. See 18 U.S.C. § 2511(2)(d) ("It shall not be unlawful . . . for a person . . . to intercept a wire, oral, or electronic communication, where such person is a party to the communication or where one of the parties to the communication has given prior consent . . ."). Thus, the scope of liability under the Federal law is significantly limited in a way that our wiretap act, which requires the consent of all parties to a communication, is not. See G. L. c. 272, § 99 B 4 (permitting interception only by "a

[33] Vita also cites Federal court opinions, most of them unpublished, interpreting other States' wiretap statutes and concluding that the statute applies to communications between a website and a user. To the extent some of the cases involve similar fact patterns, these cases interpret different State laws; also, those State laws have been amended far more recently than our wiretap act. See, e.g., Cal. Penal Code § 632.01, inserted by Cal. Stat. 2016, c. 855 (A.B. 1671) (crime to intentionally disclose or distribute, "in any forum, including . . . Internet Web sites . . . the contents of a confidential communication with a health care provider" that is illegally intercepted); 18 Pa. Cons. Stat. § 5704, as amended through 2017 Pa. Legis. Serv. Act 2017-22 (S.B. 560) ("telephone calls" and "conversations" in wiretap act replaced with "oral communication, electronic communication, or wire communication").

person given prior authority by all parties to such communication"). The Federal law therefore provides no basis for resolving the ambiguity here.

e. Rule of lenity. After examining the statute's text and legislative history, and reviewing our own case law, we are left with serious doubts as to whether browsing and interacting with a public website are a "wire communication" under the wiretap act. Accordingly, the statute is ambiguous. "Under the rule of lenity, if we find that the statute is ambiguous or are unable to ascertain the intent of the Legislature, the defendant is entitled to the benefit of any rational doubt" (citation and quotation omitted). Montarvo, 486 Mass. at 542.

While the instant cases concern civil liability under the wiretap act, the act also has significant criminal penalties, including up to five years in State prison, and accordingly, the rule of lenity should be applied. See 3 S. Singer, Statutes and Statutory Construction § 59:4 (8th ed. Nov. 2023 update) ("If a law has both criminal and civil applications, the rule of lenity governs its interpretations in both settings"). See also Leocal v. Ashcroft, 543 U.S. 1, 11 n.8 (2004) ("Because we must interpret the statute consistently, whether we encounter its

application in a criminal or noncriminal context, the rule of lenity applies").[34]

We therefore cannot conclude, in "the absence of an express textual provision or an indication of legislative intent," that browsing and other similar website interactions of the kind Vita alleges she engaged in on the hospitals' websites are "wire communication[s]" under the wiretap act. See Anderson v. National Union Fire Ins. Co. of Pittsburgh PA, 476 Mass. 377, 386 (2017). Activities such as entering a URL, accessing a specific webpage, clicking on links, and scrolling through a webpage are clearly not the type of person-to-person conversation or messaging unambiguously protected by the act. Similarly, the transmission of data about a user's web browser configuration and IP address bear little resemblance to person-to-person conversation.

We also cannot deem as communications the interception of which might lead to criminal penalties the act of simply running

---

[34] Indeed, we have explicitly applied the rule of lenity to civil statutes with no criminal component if the statutory provision was penal in nature. See Anderson v. National Union Fire Ins. Co. of Pittsburgh PA, 476 Mass. 377, 386 (2017) (applying rule of lenity to treble damages provision of civil statute, G. L. c. 93A); Libby v. New York, N.H. & H.R.R., 273 Mass. 522, 525-526 (1930) (statute providing civil damages for injuries caused by railroad collisions "must be construed strictly and not extended by equity, or by the probable or supposed intention of the [L]egislature as derived from doubtful words" [quotation and citation omitted]).

searches on the websites or accessing information about doctors published on the websites, as alleged by Vita. These interactions with a website, as explained above, differ in material respects from person-to-person conversations and messaging. The website user is interacting with the website, not another person, and accessing publicly available data, not having a personal conversation or sending a personal message.

In analyzing whether the interception of this information constitutes a criminal violation, we must keep in mind that the statute does not distinguish medical information from other information, or hospital websites from other websites.[35] Consequently, we must impose a common definition of communication of information for all websites. For example, would it be a criminal violation if a user browses a music or sports website, to inquire about particular songs or athletes, and the music website or sports website tracks its users, and shares that information with Internet advertisers without the user's consent? Under this interpretation, it would appear that thousands of website owners could potentially face severe

[35] The dissent attempts to narrow the application of Vita's interpretation to the collection of medical information. But it fails to explain why such browsing is communication when one browses a public medical website, as opposed to browsing any other type of public website. The statute certainly draws no such distinction. It is not specifically directed at medical information as opposed to any other information.

criminal and civil penalties for using tracking tools needed to support an advertising-based business model that is so common on the Internet. See Amended Opening Brief for Defendants-Appellants, at 24-25; Brief for National Retail Federation and Retailers Association of Massachusetts, as Amici Curiae, at 3 ("The technologies at issue in this case are found on all manner of websites . . .").[36]

The dissent likens the hospitals' websites to a virtual "customer service representative or healthcare provider, receiving inquiries from patients about, inter alia, a particular medical condition or specific physicians and, in exchange, providing the hospitals' response." Post at . The same can of course be said for all other businesses' websites. The dissent's interpretations would also appear to apply to automated telephone directories that ask us to dial particular numbers to access different types of information. Is each one of these interactions a wiretap violation subject to criminal penalties, including a prison sentence of up to five years, if

[36] The dissent claims we are motivated in our reasoning by "business realities." Post at note 33. To be sure, we do not ignore "business realities," as courts should, of course, take care to consider the real-world application of a proposed reading of a statute. But the principle guiding our analysis is, more simply, adherence to the rule of lenity where a criminal statute is ambiguous. Unlike the dissent, we will not impose penalties of up to five years in prison on activity that has not been clearly defined to be criminal.

it is monitored? Moreover, unlike a call to a customer service representative to seek information, there is not another person engaged in a conversation when a website user searches for or requests information, and the website provides pre-generated content that is publicly accessible.

We emphasize that Vita does not allege that her communications with a particular physician, nurse, or other medical professional were intercepted.[37] If such communications were intercepted, these would be much different cases.

We also emphasize that the Legislature has provided other statutory and common-law causes of action to address allegedly false, misleading, or deceptive activity on the Internet, including statutory and common-law protections more directly applicable to misrepresentations or misuse of private medical information. See, e.g., Doe vs. Tenet Healthcare Corp., U.S. Dist. Ct., No. 23-12978-PBS (D. Mass. Apr. 23, 2024) (plaintiff stated claims for negligence, breach of implied contract, unjust enrichment, breach of fiduciary duty, right to privacy, and G. L. c. 93A violation, where hospital website allegedly tracked and shared with third parties plaintiff's website browsing activities). For example, G. L. c. 214, § 1B, provides a "right

[37] Vita also does not allege that her or her husband's private medical records, that is, medical information prepared by doctors, nurses, or physician assistants for either of them, were transmitted to third parties without their consent.

against unreasonable, substantial or serious interference with [an individual's] privacy." Deception or misrepresentation in a privacy policy may also support a cognizable claim under G. L. c. 93A, and the powerful remedies that statute provides. See Connor v. Marriott Int'l, Inc., 103 Mass. App. Ct. 828, 836 (2024) ("An act or practice will be found deceptive if, first, there is a representation, omission, or practice that, second, is likely to mislead consumers acting reasonably under the circumstances, and third, the representation, omission, or practice is material" [quotation and citation omitted]). There are also, of course, many laws that strictly protect patient information. See, e.g., G. L. c. 111, § 70E (giving every patient or resident of medical facility right "to confidentiality of all records and communications to the extent provided by law"); 42 U.S.C. § 1320d-6(a) (crime to knowingly obtain or disclose "individually identifiable health information").

In sum, the statutory language is ambiguous, and the legislative history is not helpful regarding whether the alleged interceptions of Vita's uses of the hospitals' websites are interceptions of "communications" within the meaning of the wiretap act and thereby potentially subject to both civil and criminal penalties. Therefore, the rule of lenity applies, and Vita's claims against the hospitals, which are based on the

wiretap act alone, should be dismissed. See Commonwealth v. Constantino, 443 Mass. 521, 525 (2005) (where statute can "plausibly be found to be ambiguous" defendant should receive "the benefit of the ambiguity" [citation omitted]).

3. Conclusion. For the foregoing reasons, we reverse the Superior Court orders denying the hospitals' motions to dismiss the complaints.

So ordered.

WENDLANDT, J. (dissenting). Individuals in the Commonwealth increasingly conduct their affairs over the Internet, sharing often sensitive personal information with companies by using company websites rather than landline telephones. The defendants New England Baptist Hospital (NEBH) and Beth Israel Deaconess Medical Center, Inc. (BIDMC) (collectively, hospitals), created their own online presence to communicate with their patients, encouraging engagement with this electronic medium -- their websites -- as an alternative to the telephone for patients to obtain information from and about the hospitals, and for the hospitals to elicit information from patients related to their specific medical needs and care.

The hospitals well understood that their websites were a means to communicate privately with patients -- an inference that is not only reasonable, but almost inescapable when one reads the hospitals' representations. Mirroring protocols attendant to face-to-face interactions between healthcare providers and patients, the hospitals assured patients that they could use these platforms to share their individualized medical concerns and inquiries privately and, in turn, to receive the hospitals' tailored responses. Patients were invited to visit the hospitals' websites "without identifying" themselves; for those who "elect[ed] to provide identifiable information," the hospitals promised to "make every effort to protect [their]

privacy." Come, they told patients like the plaintiff Kathleen Vita, use our websites as a virtual space where you can share your private medical concerns, and start receiving our professional medical advice, confidentially.

Then, unbeknownst to their patients, the hospitals aided third parties to record this healthcare information, allowing the third parties to create detailed portraits of the patients' medical needs and to monetize this information for advertisements targeted to those patients. Rather than candidly disclose this arrangement, the hospitals assured patients that, on their websites, the patients' identities and privacy would be maintained. In short, the hospitals lied.

Words matter. I agree with the court that the words of a statute must be read in context, but they must be read. To be sure, the Legislature in the 1960s, when it passed G. L. c. 272, § 99 (wiretap act or act), may not have divined how the Internet would revolutionize the way we communicate. But because the Legislature chose particular words, this understandable shortcoming does not mean, as the court concludes, that the act is hopelessly ambiguous and unable to protect against the surreptitious recordings that occurred here.

Pertinent to our query, the Legislature chose the term "communication" -- specifically, "any communication" -- to define the subject matter of the act's protections (emphasis

added), G. L. c. 272, § 99 B 1; it did not limit protections to the "person-to-person conversations or messaging" that the court finds were the "core type of communication" with which the Legislature expressed specific concern, ante at . In my view, the words "any communication" leave no room for ambiguity. Where a technological advance (like the telephone before it) revolutionizes how we communicate -- by selecting dropdown filters specifying preferences to find and to book an appointment with an available physician on a website, for example, rather than doing the same by dialing a keypad and placing a call to the hospital using a telephone -- the Legislature chose to protect these new ways of exchanging information against electronic eavesdroppers.

Indeed, in an apparent attempt to avoid any lingering doubts about the protections it envisioned, the Legislature made pellucid its intent by choosing specific words, codifying them in the act's preamble. In words too clear to support any claimed ambiguity, the Legislature expressly set forth its finding

> "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." (Emphases added.)

G. L. c. 272, § 99 A. The Legislature had the clairvoyance to choose these particular words to indicate that it was the

tremendous power of electronic surveillance devices -- like the tracking software at issue in the instant cases -- to enhance the ability to snoop far beyond what could be done by the human ear alone that defined the scope of the act's protections.

The court loses sight of this aim, apparently blinded by its determination that "tracking tools [are] needed to support an advertising-based business model that is so common on the Internet," ante at , and by the stated assumption that candidly disclosing this tracking to patients threatens Facebook's and Google's bottom line, id. at . As a result, it concludes that when a patient and her physician discuss frequently asked questions regarding the symptoms and treatment options of a particular disease, either in person or by telephone, that discussion cannot be "bugged" under the act. But when the hospitals create an electronic forum to allow that same information to be exchanged over the hospitals' website, they can implant tracking code to record the discussion secretly and then sell the information to the highest bidder without recourse in the act. When a patient telephones the doctor's office to schedule an appointment, that conversation cannot be recorded secretly by a modern surveillance device under the act; but when that same exchange occurs on a website designed to facilitate such scheduling, it bewilders the court to conclude that the act extends so far. Under the court's construction (or

lack thereof), the act permits the hospitals to market their websites as purportedly private spaces for dispensing medical information on a confidential basis, and then, as alleged by Vita, to assist "silent third-part[ies] [to] watch[] whatever [their patients are] doing." I disagree.

Of course, public policy decisions regarding the protections afforded to our communications over evolving technologies against electronic surveillance by private parties need to be left to the Legislature; but once those decisions have been made and set forth in clear language, as the Legislature has done in the wiretap act, it is our function to enforce them. Because, in words too plain to question, the Legislature told us that the secret recordings alleged to have occurred here fall squarely within the threat to privacy it enacted the wiretap act to curb, and because those same words show that the Legislature intended that such secret surveillance would not escape the act's reach when it occurs over a website on the Internet rather than over a telephone or telegraph, I respectfully dissent.

1. Standard of review. "We review the denial of a motion to dismiss under Mass. R. Civ. P. 12 (b) (6)[, 365 Mass. 754 (1974),] de novo." Marsh v. Massachusetts Coastal R.R., 492 Mass. 641, 645 (2023), cert. denied, 144 S. Ct. 2519 (2024), quoting Dunn v. Genzyme Corp., 486 Mass. 713, 717 (2021). "In

doing so, we accept 'as true all well-pleaded facts alleged in the complaint, drawing all reasonable inferences therefrom in the plaintiff's favor, and determining whether the allegations plausibly suggest that the plaintiff is entitled to relief.'" Marsh, supra at 645-646, quoting Lanier v. President & Fellows of Harvard College, 490 Mass. 37, 43 (2022). See Iannacchino v. Ford Motor Co., 451 Mass. 623, 636 (2008) ("Factual allegations must be enough to raise a right to relief above the speculative level . . ." [citation omitted]).

Straying from this standard, the court focuses on certain website features that Vita "regularly" used, discussing Vita's putative failure to state with sufficient clarity whether she also was among those healthcare consumers who took advantage of each of the myriad of options made available by the hospitals on their websites. Such an application of what appears to be a heightened pleading standard, or a premature analysis of whether Vita is an appropriate class representative, is inconsistent with the liberal rules applicable to Vita's complaints. Cf. Mass. R. Civ. P. 9, 365 Mass. 751 (1974) (heightened pleading standards applicable to claims of fraud);[1] Mass. R. Civ. P. 23,

[1] For example, the court recognizes that the websites were used by a patient to communicate requests to the hospitals to book appointments and to reserve a spot in the urgent care line, but then places significance on Vita's purported failure to allege whether "users could engage in substantive written

as amended, 471 Mass. 1491 (2015) (setting forth rules for class certification). Drawing all reasonable inferences in Vita's favor, as we must on a motion to dismiss, her "regular" use of certain features on the hospitals' websites does not limit our analysis on a motion to dismiss.

2. Communication. Enacted in 1968 in response to "the uncontrolled development and unrestricted use of modern electronic surveillance devices," the wiretap act generally precludes aiding another to record secretly the "contents" of "any wire or oral communication." G. L. c. 272, § 99 A, C. A "wire communication" is defined 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" (emphasis added). G. L. c. 272, § 99 B 1.

The instant cases present the questions whether the electronic exchanges of information between Vita and the hospitals by means of the hospitals' websites constituted "communication[s]" protected against surreptitious monitoring as

---

conversations or draft particularized messages to health care providers using the forms." Ante at note 8. It is not clear why or whether that additional allegation would affect the court's analysis. Certainly, nothing in the act itself requires a communication to be particularly "substantive" or "particularized" to warrant protection. As discussed infra, the act protects "any communication." G. L. c. 272, § 99 B 1.

"wire communication[s]" by the wiretap act, and, if so, whether Vita's complaints allege that the "contents"[2] of those communications were intercepted in violation of the act.

a. Plain meaning. The word "communication" is not defined by the act. In the absence of an express statutory definition of the term, "[w]e derive the word['s] usual and accepted meanings from sources presumably known to the statute's enactors, such as [its] use in other legal contexts and dictionary definitions." Curtatone v. Barstool Sports, Inc., 487 Mass. 655, 658 (2021), quoting Commonwealth v. Matta, 483 Mass. 357, 372 (2019). See Matter of the Estate of Mason, 493 Mass. 148, 151 (2023), quoting Metcalf v. BSC Group, Inc., 492 Mass. 676, 681 (2023) ("In construing a statute, we begin with its plain language"); Garcia v. Steele, 492 Mass. 322, 326 (2023), quoting Sandifer v. United States Steel Corp., 571 U.S. 220, 227 (2014) ("words will be interpreted as taking their ordinary, contemporary, common meaning"). It is for this reason that we turn to dictionaries as the first and primary source for the construction of words that the Legislature used but left

[2] As discussed in detail infra, the act makes clear that the "contents" of a communication include more than the communication itself; it defines "contents" as "any information concerning the identity of the parties to [a] communication or the existence, contents, substance, purport, or meaning of that communication." G. L. c. 272, § 99 B 5.

undefined.[3] See Millis Public Sch. v. M.P., 478 Mass. 767, 775 (2018), quoting Commonwealth v. Samuel S., 476 Mass. 497, 501 (2017) ("We look initially 'to dictionary definitions as a guide to a term's plain or ordinary meaning'").

i. Dictionary definitions. The definition of the term "communication" is the "exchange of information, knowledge, or ideas, by means of speech, writing, mechanical or electronic media, etc." Oxford English Dictionary Online. See Black's Law Dictionary 350 (12th ed. 2024) (defining communication as "[t]he interchange of messages or ideas by speech, writing, gestures, or conduct; the process of bringing an idea to another's perception"); Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/communication [https://perma.cc/7VX3-KSG7] ("a process by which information is exchanged between individuals through a common system of symbols, signs, or behavior"); American Heritage Dictionary of the English Language 269 (1970) ("The exchange of thoughts, messages, or the like, as by speech, signals, or writing"); Random House

[3] Rather than start its analysis with this trusted resource, the court takes an unusual approach, searching the act for "examples" of communications and then declaring that in light of this sampling, the dictionary definitions are "too varied and too vague" to be useful (quotation and citation omitted). Ante at note 23. I disagree. The definitions provided by the dictionaries are neither too varied nor too vague; central to each is the exchange of information and knowledge. And, as explained infra, the samples relied on by the court comprise a subset of the broader definition of "communication."

Dictionary of the English Language 298 (1967) ("the imparting or interchange of thoughts, opinions, or information by speech, writing, or signs").

Considering these definitions, I agree with the court that the plain meaning of "communication" thus includes messages and conversations[4] between people, including by means of e-mail, text message, chat, and instant message. Ante at . However, I conclude that the term also encompasses the "exchange" of medical "information" and "knowledge" that occurred between Vita and the hospitals "by means of" the hospitals' websites on the Internet, an "electronic media."[5] See Oxford English Dictionary

---

[4] The term "conversation" means an "oral exchange of sentiments, observations, opinions, or ideas," and includes a similar exchange conducted by, for example, e-mail. Merriam-Webster Online Dictionary, https://www.merriam-webster.com/dictionary/conversation [https://perma.cc/EL4B-75K2]. Thus, a "conversation" is encompassed by the term "communication"; however, the term "communication" is broader. Cf. Commonwealth v. Zezima, 365 Mass. 238, 241 (1974) ("The adoption by the Legislature of the word 'communication' [and not 'conversation'] . . . manifests an intention to include more than conversations . . .").

[5] "[N]early everything that makes the [I]nternet function is wired. . . . Individual devices like laptops and smartphones are capable of communicating with a network (Wi-Fi or cellular network), but the routers that they connect to are almost always connected by wires." Alliance for Innovation and Infrastructure, The Infrastructure of the Physical Internet (June 27, 2023), https://www.aii.org/the-infrastructure-of-the-physical-internet [https://perma.cc/S6DL-EU2K]. See In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 501 (S.D.N.Y. 2001) ("The Internet is the physical infrastructure of the online world: the servers, computers, fiber-optic cables

Online. This plain meaning derives directly from dictionary definitions.

While the court misapprehends the hospitals' websites as repositories for "published," "pre-generated" medical data, the hospitals know better. As Vita asserts, they created the websites as confidential dynamic forums on which they communicated "interactive[ly]" with patients about the patients' "personal" medical needs. The hospitals' websites were "designed for communications with healthcare consumers," Vita contends.

It is important, then, to clarify the precise allegations that the court has labeled sweepingly as "web browsing." Vita alleges that by means of the hospitals' websites, for example, patients asked questions about physicians who met the patients' gender preferences, geographic limitations, and desired areas of specialization relevant to the patients' unique healthcare needs, and the hospitals answered by identifying available doctors to meet these specified requirements. Employing the websites, patients inquired about the hospitals' ability to

---

and routers through which data is shared online"). See also Commonwealth v. Moody, 466 Mass. 196, 198, 207 (2013) (wiretap act applies to wireless transmissions between cellular telephones because transmissions "utilize wire, cable, or other like connections, even if the use of such connections is only in switching stations").

provide specific treatments and procedures tailored to the particular maladies with which patients were afflicted; and they received the hospitals' responses. On these websites, patients completed forms and dispatched requests to the hospitals to book appointments with physicians specializing in the patients' illnesses or to reserve a spot in the urgent care line, just as they might by e-mail or by telephone.

The "private healthcare information" exchanged with the hospitals using their websites, Vita alleges, included "individual's medical conditions, doctors they might be seeing, medical searches the individual performs on the websites, and personal medical information the user enters into forms on the websites." Inconvenient as these factual allegations may be to the court's reframed narrative as to the nature of the information exchanged between patients and the hospitals over the websites, they cannot be disregarded as "embellish[ments]." Ante at note 14. Instead, because the allegations are ones of fact, I accept them as true, drawing all reasonable inferences therefrom in Vita's favor, as we must at this early stage in the pleadings. Recasting these factual allegations as "web browsing" does not alter their nature;[6] they involve exchanges of

[6] After reframing Vita's alleged exchanges of information over the hospitals' websites as "web browsing," the court casts aside dictionaries because they do not provide a "ready answer"

information over an electronic media. As such, they fall within the plain meaning of "communication."

Confirming the dictionary definitions, courts generally describe exchanges of information on the Internet between website owners and website users as "communications," applying that word's plain and ordinary meaning.[7] While not dispositive,

---

to the question whether web browsing is "with the website" or "with the website's owner." This sleight of hand does render dictionaries unhelpful in our analysis of the meaning of the term "communication," especially where the term is preceded by the word "any," as discussed infra. In any event, the information on the website did not come from the ether; the information was supplied by individuals -- representatives of the hospitals responsible for the websites' content. Accordingly, the communications alleged to have occurred here were between the hospitals and their patients by means of the hospitals' websites. See discussion infra.

[7] See, e.g., Popa v. Harriet Carter Gifts, Inc., 52 F.4th 121, 124 (3d Cir. 2022) (referring to consumer's interactions with website as "communications"); In re Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 596, 607-608 (9th Cir. 2020), cert. denied sub nom. Facebook, Inc. v. Davis, 141 S. Ct. 1684 (2021) (referring to "GET requests" between user's web browser and webpage servers, which include uniform resource locator [URL] of webpage and sometimes information about website from which user is launching new site, as "communications"); In re Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125, 130 (3d Cir. 2015), cert, denied sub nom. Gourley v. Google, Inc., 580 U.S. 814 (2016) (referring to Internet exchanges captured by "cookies," which enable transfer of information from web browser to web server, as "communications"); In re Zynga Privacy Litig., 750 F.3d 1098, 1101 (9th Cir. 2014) (describing how "communications occur between [Internet] 'clients' and 'servers'" in context of Facebook cookies transferring information); Brown v. Google LLC, 525 F. Supp. 3d 1049, 1068 (N.D. Cal. 2021) (referring to Internet exchanges captured by cookies as "communications"); In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d at 504

their use of the word "communication" to refer to these web-based exchanges of information and the absence of any confusion as to its scope bolsters the conclusion that the exchange of medical information alleged by Vita falls within the plain meaning of the term.

ii. Context. Our analysis does not end with dictionaries; words must be read in the context of the "statutory scheme as a whole." Six Bros., Inc. v. Brookline, 493 Mass. 616, 622 (2024), quoting Plymouth Retirement Bd. v. Contributory Retirement Appeal Bd., 483 Mass. 600, 605 (2019).

A. "Any communication." Significantly, the act defines the phrase "wire communication" to encompass "any communication" so long as it is transmitted, at least in part, by aid of a wire, cable, or similar connection (emphasis added). G. L. c. 272, § 99 B 1. The use of the word "any" to modify the word "communication" evinces the Legislature's intent to provide sweeping protection for communications "of whatever kind."[8] Department of Hous. & Urban Dev. v. Rucker, 535 U.S. 125, 131

(describing information exchanges between user and websites captured by cookies as "communication[s]"). See also note 23, infra (defining "cookie").

[8] Curiously, the court dismisses dictionaries as unhelpful because "the interpretive challenge comes from the ambiguity of the word as situated in [the] sentence." Ante at note 23. Yet, the court refuses to consider the word "communication" in context. Specifically, the use of the word in the sentence defining "wire communication."

(2002) ("[T]he word 'any' has an expansive meaning, that is, one or some indiscriminately of whatever kind" [quotation and citation omitted]). See Commonwealth v. Moody, 466 Mass. 196, 208 (2013) (wiretap act "define[s] 'wire communication' broadly").

This, in turn, should clarify the court's present bewilderment. The word "any" indicates the legislative intent not to limit the act's protections to direct "person-to-person" communications, to "personal" communications, to "private" communications, to "substantive" "particularized" communications or to the "core type" of communications available when the act was passed. Ante at & note 8. In this manner, the Legislature demonstrated its intent to capture new communications technologies that employ wire, cable, or other like connections even if those technologies altered the manner by which we communicate.

Dismissing this obvious statutory context and rich resource for determining legislative intent, the court instead places great weight on a subsection of the search warrant provision of the act, which uses the terms "wire and oral communications" interchangeably with "conversations," to claim puzzlement whether "communications" are limited to direct person-to-person conversations. Specifically, to obtain a search warrant authorizing the interception of a wire or oral communication,

the subsection requires that the warrant application include "[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" (emphasis added). G. L. c. 272, § 99 F 2 e. In this subtle manner, the court concludes, the Legislature might have intended to narrow the breadth of oral and wire communications, previously and expressly defined expansively to include, respectively, speech and "any communication" through the requisite medium, to conversations or messages between people such as by sending or receiving by e-mail, text message, chat, instant message, or the equivalent. G. L. c. 272, § 99 B 1.

In light of the express definition of "wire communication" and the purpose conveyed in the act's preamble to protect against the threat to privacy occasioned by modern electronic surveillance devices, discussed in further detail infra, the court is mistaken. See Patel v. 7-Eleven, Inc., 489 Mass. 356, 364 (2022), S.C., 494 Mass. 562 (2024), quoting Whitman v. American Trucking Ass'ns, 531 U.S. 457, 468 (2001) ("the Legislature 'does not, one might say, hide elephants in mouseholes'"). Instead, this singular use of the term "conversations" was intended to incorporate the breadth of the phrase "oral and wire communications," as previously discussed.

Similarly, the court concludes that, because the act uses the words "telephone" and "telegraph" several times, protected communications might be limited to direct person-to-person conversations or messages as one might conduct on a telephone or through a telegraph. Far from sowing confusion as to the scope of the phrase "any communication," these references to telephone communications and messages by telegraph show that "when the Legislature intend[ed]" to limit a provision of the act to a particular type of communication, "it [knew] how to say so explicitly" (citation omitted). Commonwealth v. Rossetti, 489 Mass. 589, 600 (2022).

Beyond requiring that the medium of exchange include, at least in part, a wire, cable, or like connection,[9] no qualifying phrase limits application of the act so as to exclude an exchange of medical information and knowledge occurring between

[9] The Legislature expressly stated its understanding that technological advances would change the ways we communicate. In describing the scope of wire communications, it chose the words "made in whole or in part through . . . wire, cable, or other like connection between the point of origin and the point of reception" to capture communications conducted over future technologies, like the Internet (emphasis added). G. L. c. 272, § 99 B 1. Faithful to that forward-looking mandate, we previously have concluded that the wiretap act applied to technologies that did not exist at the time of its enactment. See Moody, 466 Mass. at 208-209 (concluding "wire communication" includes cellular telephone calls, which only transfer through wire, cable, or like connection briefly at switching stations, as well as text messages, which are nonoral electronic communications).

a patient and a hospital by means of the hospital's website.[10] See Plymouth Retirement Bd., 483 Mass. at 605 (we "look to the statutory scheme as a whole" to derive Legislature's intent [citation omitted]). Such an exchange of information falls within "any communication."

Even if recourse to the legislative history were proper,[11] it is telling that the Legislature chose to protect "any communication" and not just the private conversations or messages discussed in the legislative record;[12] this choice to

---

[10] Indeed, both telegraph and Internet systems operate through transmission of electrical signals, leading some commentators to view telegraphs as a sort of precursor to the Internet. See generally T. Standage, The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-line Pioneers (1998).

[11] Of course, "where[, as here,] the statute is clear and unambiguous, our inquiry into the Legislature's intent need go no further than the statute's plain and ordinary meaning" (citation omitted). Commonwealth v. Mcneil, 492 Mass. 336, 337 (2023). AIDS Support Group of Cape Cod, Inc. v. Barnstable, 477 Mass. 296, 301 (2017) ("Where the language of the statute is plain and unambiguous, . . . legislative history is not ordinarily a proper source of construction" [quotation and citation omitted]).

[12] Contrary to the hospitals' argument, our opinion in Commonwealth v. Rivera, 445 Mass. 119 (2005), is not to the contrary. Expressly passing over the question whether the owner who made the recording violated the act, we concluded that suppression was not required because the State had no part in ordering or encouraging the recording. Id. at 123 ("we need not determine the predicate issue . . . whether the audiotape was made in violation of the wiretap statute"). We also mused in dicta that "the defendant cannot reasonably claim that his recorded threats and obscenities were a 'conversation'" that the

protect "any communication" must inform our construction. "We do not read into the statute a provision which the Legislature did not see fit to put there, nor add words that the Legislature had an option to, but chose not to include." Commonwealth v. Dones, 492 Mass. 291, 297 (2023), quoting Commonwealth v. Williams, 481 Mass. 799, 807-808 (2019).

Accordingly, while the Legislature was concerned principally with privacy, we have concluded that the act's protections were not limited to situations where there existed a reasonable expectation of privacy in the oral or wire communications. Commonwealth v. Hyde, 434 Mass. 594, 601 (2001), quoting Commonwealth v. Jackson, 370 Mass. 502, 506 (1976) ("[W]e would render meaningless the Legislature's careful choice of words if we were to interpret 'secretly' as encompassing only those situations where an individual has a reasonable expectation of privacy"). The same principles counsel rejection of any proposed limit of "communications" to direct person-to-person conversations or, as the court suggests, ante at , to conversations involving no "pre-generated"

---

act would protect. Id. at 127 n.10. However, we did not (and could not) thereby limit the scope of the act's protections to polite conversations.

content on the part of one of the parties to the communication.[13] See Dones, 492 Mass. at 297, quoting Williams, 481 Mass. at 807-808.

B. Preamble. Additional context informing the construction of the word "communication" comes from the act's preamble, on which we have placed particular import in connection with our construction of the act. See Commonwealth v. Rainey, 491 Mass. 632, 642 (2023) ("Where the Legislature has set forth its intent in the form of a codified preamble, we consider the preamble as part of the whole statute . . . to the extent that it does not conflict with the more specific statutory provisions").[14] See also Harvard Crimson, Inc. v.

[13] Of course, there are differences between in-person communications, telephonic communications, e-mail communications, text messages, and communications with the hospitals conducted over a website. Each technology alters the way we communicate. In some respects, the technological advances are helpful, making it possible for us to communicate over distances previously unthinkable or to place a message during nonbusiness hours seeking an appointment with a healthcare provider for our ailing loved one. In other ways, the technological advances can detract from the qualities of direct in-person interactions. However, the Legislature was clear that these differences in how we communicate would not leave the information exchange unprotected. The act protects "any" communications, even the ones that lack the personalized touch of a bygone era, and even the ones that are less substantive than others.

[14] Notably, "we have turned repeatedly to the [wiretap] statute's preamble to inform our analysis." Rainey, 491 Mass. at 642, citing Curtatone, 487 Mass. at 659-660, Commonwealth v. Tavares, 459 Mass. 289, 295 & n.5 (2011), Commonwealth v. Ennis,

President & Fellows of Harvard College, 445 Mass. 745, 749 (2006) ("a statute must be interpreted . . . in connection with the cause of its enactment, the mischief or imperfection to be remedied and the main object to be accomplished" [citation omitted]).

The preamble codifies the Legislature's intent to provide comprehensive protections to the privacy of individuals against surreptitious surveillance by private parties. It emphasizes the Legislature's concern that "the uncontrolled development and unrestricted use of modern electronic surveillance devices pose grave dangers to the privacy of all citizens of the commonwealth," and it sets forth the legislative intent that the "secret use of such devices by private individuals must be prohibited." G. L. c. 272, § 99 A. See Curtatone, 487 Mass. at 657 (act prohibits all secret interceptions subject to "a few narrow exceptions"). Narrowing the scope of the act's protections against secret eavesdropping and secret recording to exclude exchanges of information, knowledge, or ideas that occur between a patient and a hospital by means of the hospital's website would contravene the Legislature's stated purpose as codified in the preamble; the legislative purpose to protect

---

439 Mass. 64, 68 (2003), Commonwealth v. Gordon, 422 Mass. 816, 833 (1996), and Commonwealth v. Thorpe, 384 Mass. 271, 279 (1981), cert. denied, 454 U.S. 1147 (1982).

against the dangers of electronic eavesdropping is particularly relevant where, as here, that information exchange reveals potentially sensitive medical information. The preamble confirms the deliberate breadth of the language "any communication" regardless of whether the communication mirrors the manner by which telephone conversations were conducted.

Consistent with the preamble, the legislative record reveals a concern over conduct analogous to that which Vita alleges transpired here. The report of a special commission tasked with studying electronic eavesdropping and wiretapping prior to adoption of the present act suggests that the Legislature was concerned by the ease with which "newly developed inventions" permitted individuals to eavesdrop electronically. Commonwealth v. Ennis, 439 Mass. 64, 68 n.10 (2003), citing 1967 Senate Doc. No. 1198, at 3. The software-based eavesdropping tool used by the hospitals is precisely the sort of "modern electronic surveillance device[]" that the Legislature sought to prohibit. Contrary to the court's assertion, the fact that the code was deployed on a personal computing device by the hospitals despite their assurance of confidentiality is not less "frightening" than placing a bug in

a home or a telephone.[15] Ante at . Certainly, the historical review does not support the court's view that it is unclear whether the kinds of interceptions at issue here would fall within the ambit of concerns motivating passage of the act and set forth in its preamble.[16]

---

[15] I disagree with the court's conclusion that the Legislature, which was frightened by the capacity of cigarette pack-sized "parasite bugs" and by "room bugs" that could pick up a whisper from twenty feet away, ante at , would be less abhorred by "hidden code" secretly "injected" into patients' home computers that enables observers to watch from anywhere patients' healthcare communications on hospital websites, as Vita alleges.

[16] The court declares the "historic analogies" to "website analytics" to be tracking of mail order purchasing decisions, compiling of customer lists, and sharing the same. Ante at . But such manual endeavors are not "modern electronic surveillance devices" with the attendant capacity of such electronic devices to surpass what can be done manually (emphasis added). G. L. c. 272, § 99 A. It thus is not surprising that the Legislature did not discuss such basic manual business activities. By contrast, the tracking software -- indisputably a form of modern electronic surveillance device -- alleged by Vita in her complaints falls within the Legislature's area of concern.

Notably, when it enacted the statute, the Legislature was alarmed by the revelation that a telephone company was secretly monitoring and recording telephone calls between customers. Ennis, 439 Mass. at 69 n.10, citing 1967 Senate Doc. No. 1198, at 14. Secret monitoring of communications exchanged through a company's website is, in material respects, a modern-day equivalent of a telephone company secretly monitoring and recording customer's use of its landlines -- a practice that particularly concerned the Legislature. See Ennis, supra, citing 1968 Senate Doc. No. 1132, at 6-7, and 1967 Senate Doc. No. 1198, at 14 (partial motivation for wiretap act was revelation that telephone company was recording customers' calls secretly).

C. Person-to-person communications. The court asserts that a communication between a patient and a hospital using a website is not a communication between individuals in a "commonsense way," ante at ; instead, the court declares that it is an interaction "with a website," which the court describes as "published information" -- a repository for a large volume of generic medical information, id. at . But this is not how the hospitals themselves describe this online forum, and for good reason. The hospitals' websites function as interactive mechanisms through which the hospitals communicate information about, inter alia, their services and physicians to their patients and to the public at large, and the websites function as electronic forums for the hospitals to elicit information from patients concerning, inter alia, particular medical needs, to provide patients with responsive information, and to schedule appointments with specific providers.

The result is a personalized exchange of information specific to the patient's healthcare inquiries and needs. Unlike the court, the hospitals understood that their websites were a means to communicate privately with patients. Copying protocols required for face-to-face communications between healthcare providers and patients, the hospitals assured patients that they could use the websites to share their

individualized medical concerns and inquiries privately and, in turn, to receive the hospitals' tailored responses.

As amici Massachusetts Health and Hospital Association, Inc., and Massachusetts Medical Society acknowledge:

> "The [I]nternet is often the first place that patients, family members, researchers, and anyone curious about a particular medical condition or provider turn when seeking health-related information. Hospitals and health care providers seek to help individuals by providing online content designed to be responsive to those needs."

The websites, in effect, act like the hospitals' customer service representative or healthcare provider, receiving inquiries from patients about, inter alia, a particular medical condition or specific physicians and, in exchange, providing the hospitals' response in this modern medium.[17]

---

[17] One of the Internet's most significant contributions has been to make possible instantaneous communications across vast expanses. As the United States Supreme Court described:

> "Anyone with access to the Internet may take advantage of a wide variety of communication and information retrieval methods. These methods are constantly evolving and difficult to categorize precisely. . . . All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium -- known to its users as 'cyberspace' -- located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet."

Reno v. American Civil Liberties Union, 521 U.S. 844, 851 (1997).

Of course, a patient is an individual on one end of this virtual call. That individual asks for information regarding a particular disease or procedure by clicking an available hyperlink or typing in search terms. She asks to book an appointment by filling out a form on the website.

On the other end of the "call," there are also individuals. These are the employees and representatives of the hospitals, who are knowledgeable about, for example, the diseases or procedures that were the subject of the patient's inquiry and who are responsible for creating the answers to patients' frequently asked questions. They are the hospitals' agents who provide the information necessary to take the unique wishes of the individual patient and to develop an algorithm to provide the responsive list of qualified physicians. They are the hospitals' representatives who can take the patient's appointment request form and book the appointment with the requested physician or the individuals at the hospitals responsible for urgent care.[18] The information on the hospitals' websites does not create itself; it is designed by humans acting

[18] As described supra, the fact that the hospitals' responses are, in some sense, pre-generated is not dispositive; nothing in the act limits its protection of "any communication" to spontaneous or extemporaneous communications. Cf. Armata v. Target Corp., 480 Mass. 14, 19-20 (2018) (automatically dialed and delivered prerecorded telephone message constituted "communication" under debt collection regulation).

on the hospitals' behalf. Indeed, the hospitals do not argue to the contrary.

In short, the hospitals' websites are, by design, the hospitals' "voice" to the public and to patients on the Internet; to interact with the hospitals in this forum, patients, inter alia, direct their web browsers to launch the hospitals' websites, click on hyperlinks related to the information they seek, type in search terms to garner more information, select filters or enter searches to identify doctors, or fill out forms to request an appointment or to reserve a spot in the urgent care line. Thus, like dialing the hospitals' main telephone number on a telephone keypad to enter the signals required to call the hospital, talking into the handset, and then being directed to a customer service representative to find, for example, the closest physician of a particular gender who specializes in fertility issues, the website fields that same "call" from Internet users.[19]

The court's conclusion that the communications alleged by Vita are "with the websites" is no more supportable than a

---

[19] Accord Revitch vs. New Moosejaw, LLC, U.S. Dist. Ct., No. 18-cv-06827-VC (N.D. Cal. Oct. 23, 2019) ("request[ing] information . . . by clicking on items of interest" and receiving that information in response is akin to "call[ing] to inquire about a store's products," and "[t]his series of requests and responses -- whether online or over the phone -- is communication").

conclusion that a communication conducted by dialing a hospital's telephone number on a keypad is "with a telephone." Both sets of communications are with the hospitals, regardless of how the technological advance connects patients to the hospitals; both are encompassed by the phrase "any communication."[20]

---

[20] Deviating from our standard of review on a motion to dismiss, which requires us to draw all reasonable inferences in the plaintiff's favor, see supra, the court appears to rely on Vita's characterization of her "intercepted communications" as being between Vita and "each hospital's website." Ante at . If Vita's allegations are to be controlling, then, at the least on a motion to dismiss, we must consider her numerous allegations describing the use of the website features as communications with the hospitals. See, e.g., Vita vs. Beth Israel Deaconess Med. Ctr., Inc., Mass. Super. Ct., No. 2384CV00480, Complaint ¶ 1 (Suffolk County Feb. 24, 2023) (BIDMC Complaint) ("Plaintiff brings this action to remedy the secret interception of the contents of [I]nternet communications between healthcare consumers and the defendant, [BIDMC]. . . . The Plaintiff's and Class Members' wire communications with BIDMC were secretly and contemporaneously intercepted, recorded, and transmitted to these third parties without their knowledge or consent whenever they visited any page of the BIDMC Website"); BIDMC Complaint ¶ 7 ("this case concerns communications between healthcare consumers and healthcare providers"); BIDMC Complaint ¶ 9 ("BIDMC aided interceptions by . . . third parties of healthcare consumers' communications with BIDMC through the BIDMC Website"); BIDMC Complaint ¶ 18 ("Users of healthcare-related websites such as the BIDMC Website have a legitimate expectation and understanding that their communications with BIDMC through the website will be private. They also have a legitimate expectation that healthcare providers such as BIDMC will not share with third parties their communications with BIDMC without their consent"); BIDMC Complaint ¶ 20 ("Healthcare consumers would not anticipate or expect that their communications with healthcare providers, including BIDMC, which reveal information about that

individual's personal health conditions, will be intercepted and secretly shared . . ."); BIDMC Complaint ¶ 25 ("The interceptions of website users' communications with BIDMC were, therefore, truly secret . . ."); BIDMC Complaint ¶ 26 ("Plaintiff describes in this complaint various tracking technologies implemented on the BIDMC Website that cause the secret interception, recording, and transmission of the contents of Class Members' [I]nternet communications with BIDMC. The next section . . . provides a brief overview of the third parties that intercept and record the contents of Class Members' [I]nternet communications with BIDMC . . ."); BIDMC Complaint ¶ 38 ("BIDMC injects hidden code into the BIDMC Website that permits third parties to contemporaneously intercept healthcare consumers' communications with BIDMC. . . . This includes, for example, associating the content of the user's communications with BIDMC with the website user's Facebook profile"); BIDMC Complaint ¶ 39 ("These tracking technologies transmit to [third parties] contemporaneously with the website communications between Class Members and BIDMC, the contents of those communications and identifying information about the Class Members"); BIDMC Complaint ¶ 50 ("A third party . . . can then add the content of the user's communications with BIDMC to its collection of information it already has about the individual, which it can then use for advertising purposes"); BIDMC Complaint ¶ 52 ("The tracking technologies described in this complaint intercept and transmit to third parties the contents of communications between healthcare consumers and BIDMC contemporaneously with those communications"); BIDMC Complaint ¶ 54 ("These tracking technologies are each substantially similar to the now-removed [third party] code, both in their surreptitious deployment on the website and their contemporaneous interception of website users' communications with BIDMC"); BIDMC Complaint ¶ 63 ("After [a third party] associates the website user's communications with BIDMC with the identity of particular individuals known to [the third party], [the third party] can use that information for its own commercial purposes . . ."); BIDMC Complaint ¶ 66 ("Below is an example of the contents of the communication between the website user and BIDMC, which the hidden [code] would intercept and transmit to [a third party]"); BIDMC Complaint ¶ 68 ("With that information, [a third party] could then use the contents of communications between the website user and BIDMC to serve personalized advertising to the website user in the future") (Emphases added.). The above is exemplary; other allegations are the same and repeated with regard to NEBH.

b. Personal communications. The hospitals posit that Vita's complaints merely describe the recording of her "movements in digital space," not exchanges of information. For its part, the court concludes that Vita's "browsing activities" were not "personal." Ante at . These arguments misapprehend the crux of Vita's claims.

Her claims do not center on the tracking of the Cartesian coordinates or pixel locations on her electronic device's screen where she moved her cursor and "clicked," or the keyboard strokes she entered as she typed words into the hospitals' website search engines. Instead, her claims rest principally on the personal information exchanged between her and the hospitals.

That information comprised, inter alia, the particular type of healthcare information that Vita sought and that the hospitals provided on the webpages to which she was directed in response to her inquiries; the search terms she typed into the hospitals' website search bars to garner information regarding her and her husband's medical conditions, symptoms, and treatment, and the hospitals' responses to the same; her inquiries as to the hospitals' available physicians based on gender preferences, geographic limitations and specialization, and the hospitals' answers listing the physicians that fit her criteria and the types of maladies in which they specialized;

the specific providers with whom she sought medical services; her intent to pay or view a medical bill; and her requests to schedule appointments or be seen by an urgent care provider.

Indeed, the value of the information that the hospitals allegedly assisted the third-party software providers secretly to record lies presumably in the rich portrait of Vita garnered from the treasure trove of information Vita and the hospitals exchanged during her interactions with the hospital websites. Recasting these exchanges as mere "digital movements," as the hospitals do, or concluding that they involve no "personal" information, as the court does, ignores the reality of the information that the hospitals assisted third-party software providers to track secretly.[21] As described in the complaint, the hospitals allowed the third-party software providers to be "silent third-part[ies] watching whatever [Vita was] doing." Assuming arguendo that the act includes an unstated requirement

[21] The tracking software captured information about Vita's and her husband's medical conditions and care. As an example, Vita posited that if she navigated to the hospitals' webpages concerning pregnancy treatments, queried the websites with pregnancy-related search terms, requested an appointment with the obstetrics department, entered the payment portal, or accessed the patient portal, the data collected by the software could be employed to discern that Vita or someone she knows was pregnant and was receiving care from physicians affiliated with the hospitals. In combination with other information known about Vita, the third-party software providers thereafter could monetize this information to sell and deliver targeted digital advertisements regarding pregnancy or prenatal care to Vita.

that the communication secretly recorded is a "personal" one, Vita's allegations meet it.

c. Prior determination of act's scope. The court asserts that an amendment to the act is required to capture the interception that occurred here in order for our State act to mirror the breadth of the Federal wiretap statute, 18 U.S.C. §§ 2510 et seq. But we previously have concluded that our State act's protections of "communication[s]" is coextensive with the Federal counterpart without amendment; we explained that, even unamended, our act extends to "non-oral electronic transmissions" covered by the Federal counterpart as "electronic communications" -- a category of protected communications that Congress added in connection with the amendments to the Federal act as part of the Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (1986).[22] Moody, 466

[22] The ECPA narrowed the Federal wiretap act's definition of "wire communication" from one that essentially was identical to our State wiretap act's definition of "wire communication" by substituting the phrase "any aural transfer" for "any communication," thereby limiting wire communications under the Federal statute to those involving the human voice. Pub. L. No. 99-508, § 101(a)(1)(B), 100 Stat. at 1848, codified, as amended, at 18 U.S.C. § 2510(1). See Moody, 466 Mass. at 202-203. At the same time, however, the ECPA defined a new category called "electronic communications," which includes "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system" but not oral or wire communications as redefined in the amended Federal act. Pub. L. No. 99-508, § 101(a)(6)(B), 100 Stat. at 1848-

Mass. at 208. See id., quoting Dillon v. Massachusetts Bay Transp. Auth., 49 Mass. App. Ct. 309, 315 (2000) ("The fact that there has been no amendment of the Massachusetts [wiretap] statute comparable to the Congressional action of 1986 does not bar us from reading the [Massachusetts wiretap statute] so as to preserve it in its intrinsic intended scope and maintain its viability in the broad run of cases . . .").

Today, the court reverses course. It states that our holding in Moody was based on the ground that text messages mirror person-to-person conversations by telephone or messages by telegraph. Ante at . But this was not the basis for our holding in Moody. Instead, that decision was grounded in our conclusion that the State act was as expansive as the amended Federal counterpart, a necessary element of our analysis of the defendant's argument that the State act was otherwise preempted by the Federal act. In so holding, we relied on the definition of wire communication extending to "any communication" as well as the State act's use of the term "record." Moody, 466 Mass. at 208-209. We did not rely, as the court now states, on whether a human was directly on either side of a text message.

1849, codified, as amended, at 18 U.S.C. § 2510(12). See Moody, supra at 202. The State act's definition of "wire communication" has not changed and has not been narrowed to mirror the Federal statute; it continues to cover "any communication" by the requisite means.

See generally id. Critical to our decision that text messages were covered by "wire communication" was our determination that that term encompassed "non-oral electronic transmissions" covered by the Federal counterpart. Id. at 208.

Given our prior determination in Moody, it is significant that the court concludes, as have some Federal courts, that under the Federal statute, third-party interceptions that occur in the course of a user's interactions with a website, like those alleged in Vita's complaints, are prohibited recordings of protected communications. See, e.g., In re Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 596, 608 (9th Cir. 2020), cert. denied sub nom. Facebook, Inc. v. Davis, 141 S. Ct. 1684 (2021) (plaintiffs stated claim under Federal wiretap act where Facebook installed "plug-in" software that collected uniform resource locator [URL] information, which "provides significant information regarding the user's browsing history, including the identity of the individual [I]nternet user and the web server, as well as the name of the web page and the search terms that the user used to find it"); In re Pharmatrak, Inc., 329 F.3d 9, 18 (1st Cir. 2003) (defendant who collected information on customers through "cookies"[23] "appropriate[ly]"

[23] A cookie is a data file received on a computer at the time that the computer's user visits a webpage and is used to record and maintain information about the user's online

did not contest "whether it . . . obtained the contents of an electronic communication" under Federal wiretap act).[24]

Consistent with our decision in Moody and the decisions of Federal courts interpreting the Federal counterpart, the term "communication" includes online exchanges of medical information between a hospital and its patients by means of the hospitals' website. As we have recognized, the Legislature chose to enact a statute that was more protective than the Federal counterpart and comparable statutes in other States,[25] rejecting proposals

---

activity. See U.S. Auto Parts Network, Inc. v. Commissioner of Revenue, 491 Mass. 122, 125 & nn.6-8 (2022).

[24] Amici Greater Boston Chamber of Commerce and Massachusetts Nonprofit Network contend that Vita's website interactions are not protected, citing Federal cases concluding that "contents" of a communication were not intercepted where recorded URLs did not "convey substantive information" but instead conveyed "mere dialing, routing, addressing, or signaling information" (quotation and citation omitted). In re Nickelodeon Consumer Privacy Litig., 827 F.3d 262, 275 (3d Cir. 2016), cert. denied sub nom. C.A.F. v. Viacom Inc., 580 U.S. 1048 (2017). The Federal statute, however, defines "contents" of a communication as only "any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). By contrast, our State counterpart defines "contents" to include "any information concerning the identity of the parties to such communication or the existence, contents, substance, purport, or meaning of that communication" (emphases added). G. L. c. 272, § 99 B 5.

[25] Courts interpreting other States' wiretap acts also have concluded that their State act applies to communications transmitted over websites on the Internet. See, e.g., Popa, 52 F.4th at 133 (Pennsylvania's wiretap statute, which models Federal wiretap statute, protected consumer's browsing activities on website); Javier vs. Assurance IQ, LLC, U.S. Ct.

that would narrow protections.[26] See Hyde, 434 Mass. at 599 ("The commission [charged with restructuring the Commonwealth's wiretap statute] clearly designed the 1968 [wiretap act] to create a more restrictive electronic surveillance statute than comparable statutes in other States").

d. Absurdity. Notably, although the court's decision rests on its determination that "communication" is an ambiguous term and although the court uses that determination to justify its application of the rule of lenity, the court relies on several cases concluding that the act is not ambiguous, but instead literally reads on certain conduct. Ante at .

App., No. 21-16351 (9th Cir. May 31, 2022) ("Though written in terms of wiretapping, [§ 631(a) of California's statute, which, like the Commonwealth's act, does not separately define electronic communications,] applies to Internet communications"); Smith vs. Google, LLC, U.S. Dist. Ct., No. 23-cv-03527 (N.D. Cal. June 3, 2024) (denying motion to dismiss claim under California wiretap statute where third-party tracking tools recorded information exchanges through website). See also McCulley vs. Banner Health, U.S. Dist. Ct., 23-cv-00985 (D. Ariz. May 10, 2024) (sustaining claim for violation of California wiretap statute where healthcare provider enabled third parties to record search terms plaintiff used to research "specific doctors and medical treatments").

[26] For example, unlike many other States' wiretap statutes, the act generally requires consent of all parties to the communication. See G. L. c. 272, § 99 (prohibiting secret recording without prior authority by all parties to communication); Hyde, 434 Mass. at 599 (act requires consent of all parties). For this reason, the hospitals are wrong to suggest that they may secretly record patient communications and then share those communications with third parties; such recording by the hospitals would be permissible only with the patient's express or implied knowledge.

Setting aside this analytical misstep, I agree with the court that, in the cited cases, we have eschewed the literal construction because doing so resulted in an absurdity unsupported by the legislative goals of the act. Cf. Commonwealth v. Morris, 492 Mass. 498, 505-508 (2023) (act does not require suppression of audiovisual recording of voluntary statement where defendant knew police were recording his statement in writing); Rainey, 491 Mass. at 642-644 (no suppression of body-worn camera recording of witness's statement where witness called police to report assault by defendant and knew her statement was being recorded in writing); Commonwealth v. Gordon, 422 Mass. 816, 832-833 (1996) (act did not require suppression of purely administrative booking video recording where it was not used as investigative tool).

However, these cases do not control our analysis here. Given the Legislature's focus on the threat to personal privacy occasioned by the use of modern electronic devices to surveil surreptitiously individuals' communications, see G. L. c. 272, § 99 A, I disagree with the court's implicit determination that the Legislature would regard as absurd holding hospitals liable when they misstate how communications between a patient and her healthcare providers would be used and shared with third parties.

Consistent with its plain meaning as well as the context of

the statutory framework as a whole, the meaning of "communication" extends to the exchange of medical information and knowledge, through speech,[27] writing, mechanical or electronic media, or equivalent means.

e. Contents. Significantly, the court confuses the act's protections of the "contents" of a communication with the "communication" itself. As discussed supra, the complaints allege that the hospitals assisted third parties to record detailed personal information exchanged between the hospitals and their patients. The act prohibits the secret recording of these communications, but it also protects their "contents," a term defined as "any information concerning the identity of the parties to [a] communication or the existence, contents, substance, purport, or meaning of that communication." G. L.

---

[27] Amici New England Legal Foundation and Associated Industries of Massachusetts suggest we construe "communication" to mean "speech," which is how the act defines "oral communication." G. L. c. 272, § 99 B 2. If the Legislature had intended "communication" also to mean "speech," it would have used the same words. Moreover, if the Legislature intended "wire communication" to be limited to speech over a wire, cable, or other like connection, as the amici suggest, it would have said so. Its choice instead to use the phrase "any communication" in the definition of "wire communication" evinces the Legislature's intent that "wire communication" be more expansive than "speech" over a wire, cable, or other like connection. See, e.g., Commonwealth v. Williamson, 462 Mass. 676, 682 (2012), quoting Ginther v. Commissioner of Ins., 427 Mass. 319, 324 (1998) ("Where the Legislature used different language in different paragraphs of the same statute, it intended different meanings").

c. 272, § 99 B 5. Thus, the "contents" impermissibly recorded included Vita's underlying communications with the hospitals as well as, inter alia, the existence of the communications, the URLs of the specific webpages she visited, the titles of the webpages through which she scrolled, the hyperlinks on which she clicked, data about her web browser configuration, the unique identifier used to track individuals across the website, and her Internet protocol address.[28]

The court states that these latter "activities" do not resemble person-to-person conversations. Ante at . Regardless, they are "information concerning the identity" of Vita and "the existence" of the communications. As such, they are protected as "contents" of the underlying communication. G. L. c. 272, § 99 B 5.

3. Interception. Concluding that Vita did not allege any communication, the court does reach the question whether an interception occurred. The hospitals contend that Vita's complaints failed to allege that she did not know that third parties were monitoring and recording the communications over the hospitals' websites, and that therefore no interception of

[28] Given the defined term "contents" in the act, the court is wrong to focus on whether Vita alleges "her husband's medical records or the contents of his patient portal were in any way collected, intercepted, and transferred to third parties." Ante at . "Contents," under the act, is clearly not so limited.

her communications occurred.[29] More specifically, the hospitals assert that Vita had actual knowledge of the recordings because their privacy policies stated, "We and our Third Party Service Provider collect and save the default information customarily logged by worldwide web server software."[30]

The argument ignores the assurances also set forth in the hospitals' privacy policies that information on user activity "is not shared with other organizations" and that "we will not share any information we receive with any outside parties."[31]

---

[29] An interception occurs only where a party "secretly hear[s], secretly record[s], or aid[s] 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.

[30] Notably, the hospitals disregard that the disclosures further provided that the logged information will only be used "to prevent security breaches and to ensure the integrity of the data on our servers" (emphasis added). Here, Vita alleges that her interactions with the hospitals were used for advertisement purposes, beyond the scope of the disclosed use. See In re Pharmatrak, Inc., 329 F.3d at 19, quoting Gilday v. DuBois, 124 F.3d 277, 297 (1st Cir. 1997) ("A party may consent to the interception of only part of a communication or to the interception of only a subset of its communications. . . . 'Thus, a reviewing court must inquire into the dimensions of the consent and then ascertain whether the interception exceeded those boundaries'" [quotation omitted]).

[31] The hospitals' reliance on our decisions in Rainey, Morris, and Curtatone is misplaced. In Rainey and Morris, each aggrieved party was on notice that the other party to the respective communication was recording the statement in some manner. Morris, 492 Mass. at 505-507. Rainey, 491 Mass. at 643-644. Similarly, in Curtatone, the aggrieved party knew that

See In re Pharmatrak, Inc., 329 F.3d at 21 ("Deficient notice will almost always defeat a claim of implied consent"). Moreover, Vita alleges that tracking software was invisible to the average website user and not otherwise apparent to her.[32] These allegations plausibly suggest that Vita was unaware that the hospitals were assisting others to record the contents of the information she exchanged with the hospitals over their websites.

The hospitals also maintain that no interception transpired because "[i]t is common knowledge in the 2020s that websites cannot follow users' browsing commands without logging (i.e., 'recording') them[and] [t]hat is how the [I]nternet inherently works." Under the hospital's theory, "every online communication would provide consent to interception by a third party." In re Pharmatrak, Inc., 329 F.3d at 21. To defeat a wiretap act claim, however, the aggrieved party must have had actual knowledge of the recording. See Jackson, 370 Mass. at 507. While the actual knowledge may be express or implied,

---

the person with whom he was speaking was recording the conversation. Curtatone, 487 Mass. at 655-658. Here, Vita alleges that she lacked notice that third parties were intercepting her communications at all.

[32] Moreover, as alleged in the complaints, even if a user used her browser settings to disable cookies, the tracking software would continue to record the user's communications with the hospitals.

constructive knowledge is insufficient. See id. Cf. In re Pharmatrak, Inc., supra at 19 ("Consent may be explicit or implied, but it must be actual consent rather than constructive consent"); Williams v. Poulos, 11 F.3d 271, 281 (1st Cir. 1993) ("Implied consent is not . . . constructive consent"). Here, nothing in the complaints' allegations, which we must accept as true at this stage in the proceedings, suggests that Vita had actual knowledge that third parties were tracking her activities. See Six Bros., Inc., 493 Mass. at 618.

The court's refusal to conclude that Vita has alleged "any communication" with the hospitals over their websites appears driven in large part by the potential exposure of other website owners who employ web analytics -- tracking software that monitors how users interact with a website to improve its delivery of information. Ante at . Of course, if those website owners candidly disclosed such tracking, then the recording would not be secret and thus would not fall within the scope of the prohibited interceptions.[33] The act prohibits

[33] Taking what appears to be judicial notice of "thousands" of websites that apparently do not disclose candidly their practice of sharing their tracking of website users' activities for advertisement purposes, the court states that it is up to the Legislature to analyze the business realities. Ante at . But the Legislature has demonstrated that when so-called business realities require a narrow exception to the act, it has provided the same. See, e.g., St. 1998, c. 163, §§ 7, 8 (amending act to exempt financial institutions' recording of

secret recordings, not disclosed ones.[34] Curtatone, 487 Mass. at 658 ("the definition of interception provided in the act requires that an interception of the type prohibited must be [1] secretly made and [2] without prior authority by all parties" [quotation and citation omitted]). G. L. c. 272, § 99 B 4 (interception occurs only where hearing or recording is "secret"). Here, however, the hospitals' disclosures are not forthright;[35] together with Vita's asserted lack of knowledge, the disclosures do not provide a defense that can be determined at this stage of the litigation.

4. Ordinary course of business exception. Because the court concludes that no communications occurred between the hospitals and Vita, it does not reach the hospitals' contention

---

telephone calls "with corporate or institutional trading partners").

[34] The court also appears to be concerned about the potential criminal liability under the act, especially for companies unaware of tracking on their websites. Ante at . Of course, the act criminalizes only "willful[]" recordings. G. L. c. 272, § 99 C 1.

[35] Nor can the hospitals credibly claim surprise. At the least, it would appear that the now two decades old decision in In re Pharmatrak, Inc., 329 F.3d at 18, might have provided notice. Indeed, the mishandling of private healthcare information has garnered the attention of the Federal Trade Commission (FTC), including some enforcement action prior to the filing of Vita's complaints. See, e.g., Matter of Flo Health, Inc., FTC File No. 1923133 (FTC enforcement action brought in January 2021 involving disclosure of health data to third-party analytics providers).

that the tracking software falls within an exception to the prohibition on "intercepting device[s]"[36] that applies to "any telephone or telegraph instrument, equipment, facility, or a component thereof" that the hospitals used "in the ordinary course of [their] business." G. L. c. 272, § 99 B 3.

To be sure, the act prohibits only interceptions that are conducted through an "intercepting device." G. L. c. 272, § 99 B 4. An intercepting device is

> "any device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire or oral communication other than . . . any telephone or telegraph instrument, equipment, facility, or a component thereof, . . . 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 . . ." (emphases added).

G. L. c. 272, § 99 B 3. Thus, certain telephone or telegraph equipment used in the ordinary course of business is exempted from the definition of an intercepting device. The hospitals do not contend that the tracking software is "telephone or telegraph equipment." See O'Sullivan v. NYNEX Corp., 426 Mass. 261, 265 (1997), quoting Commonwealth v. Todisco, 363 Mass. 445, 452 (1973) ("'telephone equipment' does not include

---

[36] The argument of amicus Chamber of Commerce of the United States of America that the tracking software does not comprise an "intercepting device" ignores that the software runs on physical infrastructure, which is a "device or apparatus which is capable of transmitting, receiving, amplifying, or recording a wire or oral communication." G. L. c. 272, § 99 B 3.

eavesdropping devices external and extraneous to regular telephone devices"). They ask us to construe "telephone and telegraph instrument" to include the tracking software at issue here. But the Legislature chose to limit expressly the exception to "any telephone or telegraph instrument." This contrasts sharply with the Legislature's decision to define "wire communication" expansively to include technologies beyond telephone and telegraph instruments. Compare G. L. c. 272, § 99 B 3, with G. L. c. 272, § 99 B 1 ("wire communication" extends to communications over "wire, cable, or other like connection"). See Commonwealth v. Williamson, 462 Mass. 676, 682 (2012) (Legislature's choice of different words demonstrates intent for different meanings).

Moreover, Vita's complaints aver that the hospitals' ordinary course of business is caring for and treating patients; it does not appear to extend to permitting third parties to exploit communications between a patient and the hospitals concerning the patient's medical inquiries, physicians, and medical care. See Crosland v. Horgan, 401 Mass. 271, 275 (1987), quoting Watkins v. L.M. Berry & Co., 704 F.2d 577, 582 (11th Cir. 1983) ("in light of the statutory purpose of protection from invasions of privacy, neither the concept of legitimate business purpose nor 'ordinary course of business' can 'be expanded to mean anything that interests a company'").

5. Conclusion. In sum, the hospitals created websites to communicate with their patients, inviting patients to share their personal medical needs and, in turn, providing the hospitals' responses. The hospitals assured patients that these exchanges of information would be kept confidential. Then, unbeknownst to patients, they implanted tracking code to assist third parties to record the patients' private medical concerns, padding Facebook's and Google's bottom lines. The court decides that the wiretap act provides no recourse despite its prohibition on surreptitious electronic surveillance by private parties. Lamentably, the court is right about one thing; the Legislature will need to correct today's error.