COMMONWEALTH OF MASSACHUSETTS

SUFFOLK, ss. **SUPERIOR COURT**
Civil No. 22-2509-BLS1

JOE ALVES[1]
Plaintiff

vs.

BJ's WHOLESALE CLUB, INC
Defendant

MEMORANDUM AND ORDER ON MOTION TO DISMISS

Plaintiff Joe Alves brings this class action to challenge the alleged use by BJ's Wholesale Club, Inc. ("BJ's") of Session Replay Code ("SRC") to record visitors' activity on its website. Alves asserts that use of the code violates the Massachusetts Wiretap Statute, G.L. c. 272, § 99, and is an invasion of privacy actionable under G.L. c. 214, § 1B. BJ's moves to dismiss the Complaint for failure to state a claim. For the following reasons, the motion must be denied.

BACKGROUND

The following background (other than footnote 2) is taken from plaintiff's Class Action Complaint ("Complaint").

SRC is a JavaScript computer code that, when embedded on a website, enables website operators to record, save, and replay visitors' interactions with the website. SRC provides online marketers and website designers with insights into the user experience. Typically, the server receiving the data from the code is controlled by a third-party Session Replay Provider ("SRP"), rather than the owner of the website where the code is embedded. SRC goes well beyond normal

[1] On behalf of himself and all others similarly situated.

website analytics. It allows the capture and recording of nearly every action a visitor takes while visiting a website, including mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry, and other forms of a user's navigation and interaction on the website. Recording this data permits SRPs to create a reenactment of a user's visit to the website in the form of a video. Typical analytic services that provide aggregate statistics do not do this.

SRC does not necessarily anonymize user sessions. Personally identifiable information typed by the website visitor and displays of user account information to a logged-in user can be captured by the code. SRPs often create "fingerprints" unique to a particular user's combination of computer and browser settings, screen configuration, and other detectable information. This fingerprint may be collected across all sites that the SRP monitors. If a user identifies themselves to one of these websites (e.g., by filling out an on-line form), the SRP can associate the fingerprint with the user's identity and back reference the user's other browsing activity. In addition to fingerprinting, SRPs also sometimes offer website owners cookie functionality that permits linking a session to an identified user.[2]

[2] A quick search on the Internet reveals the existence of a number of SRC providers and considerable information about the many uses of session replay software. See, e.g., "The definitive guide to session reply" (Mar. 25, 2023) ("Session replay capabilities elevate traditional web analytics tools by showing a complete picture of the user on a website or app."), available at https://www.fullstory.com/session-replay/; "Top 7 session replay tools for analyzing user behavior," (Feb. 28, 2023) ("A session replay, also known as a session recording, is a rendering of a user's journey through your website. Session replays show you what individual users saw and how they experienced your site during their visit—including their clicks, page scrolls, and mouse movements."), available at https://www.hotjar.com/blog/session-replay-tools/; Matsakis, L., "Over 400 of the World's Most Popular Websites Record Your Every Keystroke, Princeton Researchers Find," (Nov. 20, 2017) ("third-party scripts that run on many of the world's most popular websites track your every keystroke and then send that information to a third-party server"), available at https://www.vice.com/en/article/59yexk/princeton-study-session-replay-scripts-tracking-you. The Internet also reflects growing legal interest in litigation surrounding the use of SRC. See, e.g., Stegmaier, G, Quist, M., & Bart, A., "Lawsuits Accusing Online Session Replay of Criminal 'Wiretapping' Implicate Serious Constitutional Concerns," Washington Legal Foundation (Apr. 28, 2023), available at https://www.wlf.org/2023/04/28/

BJ's operates brick and mortar stores and a website that sells grocery items, electronics, furniture, and other products. It has embedded SRC from various SRPs on its website. The SRC operates unbeknownst to the website's visitors, to track those visitors' "mouse movements, clicks, keystrokes (such as text being entered into an information field or text box), URLs of web pages visited, and/or other electronic communications in real-time."[3] Defendant's SRPs create video replays of the behaviors of visitors to defendant's website and provides it to BJ's for analysis.

In late 2021 and early 2022, plaintiff visited defendant's website on his computer and cell phone to shop for tires. His activity was captured using the website's embedded SRC and sent to various SRPs.

DISCUSSION

I. The Rule 12(b)(6) Standard

On a motion under Mass. R. Civ. P. 12(b)(6), I must accept as true the factual allegations in the complaint and draw "all reasonable inferences" from those allegations in favor of plaintiff.

---

publishing/lawsuits-accusing-online-session-replay-of-criminal-wiretapping-implicate-serious-constitutional-concerns/; "Litigation Minute: Pennsylvania and Florida Emerge as Fertile Ground for Session Replay Litigation," The National Law Review (Apr. 18, 2023), available at https://www.natlawreview.com/article/litigation-minute-pennsylvania-and-florida-emerge-fertile-ground-session-replay; Bilus, A, Lipchitz, J. & Burdette, A., "Tips for Protecting Your Business from Wiretap Lawsuits Targeting Companies with Consumer-Facing Websites," American Bar Association (Feb. 22, 2023), available at https://www.americanbar.org/groups/litigation/committees/privacy-data-security/practice/2023/tips-protecting-business-wiretap-lawsuits/; Coyer, C., "Session Replay Software Again Faces Legal Challenges, But Likely Not for Long," Law.com (Sept. 16, 2022), available at https://www.law.com/legaltechnews/2022/09/16/session-replay-software-again-faces-legal-challenges-but-likely-not-for-long/. All links were last viewed June 21, 2023.

[3] The SRC provided by Microsoft Corporation, one of BJ's SRPs, generates basic information about website user sessions, interactions, and engagement, and breaks down users by device type, country, and other criteria.

Dunn v. Genzyme Corp., 486 Mass. 713, 717 (2021). While the factual allegations in a complaint need not be detailed, they must set forth the basis for plaintiff's entitlement to relief with "more than labels and conclusions," Iannacchino v. Ford Motor Co., 451 Mass. 623, 636 (2008), quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 555 (2007); and must "'be enough to raise a right to relief above the speculative level[,]' . . . 'plausibly suggesting (not merely consistent with)' an entitlement to relief." Iannacchino, 451 Mass. at 636 (internal citations omitted), quoting Bell Atl., 550 U.S. at 555, 557. I address each count of the Complaint in turn.

II. Massachusetts Wiretap Statute (Count I)

Count I asserts that defendant's use of SRC violates the Massachusetts Wiretap Statute, G.L. c. 272, § 99(Q), which provides a remedy for "[a]ny aggrieved person whose oral or wire communications were intercepted, disclosed or used . . . or whose personal or property interests or privacy were violated by means of an interception," unless the interception was permitted under the Wiretap Statute.[4] See Commonwealth v. Ennis, 439 Mass. 64, 68 (2003) (Wiretap Statute "sought to curtail [ ] 'grave danger[ ]' of 'the uncontrolled development and unrestricted use of modern electronic surveillance devices,' which the Legislature termed a danger 'to the privacy of all citizens.'"), quoting G.L. c. 272, § 99(A). BJ's argues that plaintiff has failed plausibly to allege that its conduct concerned wire communications or amounted to an interception.[5] I disagree.

[4] Plaintiff does not claim that defendant's SRC intercepted oral communications.

[5] Although Section 99(Q) also prohibits use or disclosure of wire communications (not simply interception), plaintiff's claim primarily focuses on defendant's interception of his data. Defendant's argument likewise focuses on whether its purported use of SRC resulted in an interception. BJ's argues that plaintiff failed to plead use or disclosure with sufficient particularity, a position plaintiff contests. Because I conclude that plaintiff has plausibly alleged that an interception occurred, I need not address defendant's additional argument.

A. Wire Communication

The Wiretap Statute defines a "wire communication" as "any communication made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception." G.L. c. 272, § 99(B)(1). BJ's argues that plaintiff's Complaint does not implicate "wire communications" because the alleged Internet-based interactions (i) are not communications, and (ii) do not involve use of "a wire, cable, or other like connection." At this pleading stage, I am not persuaded this is correct.

The Wiretap Statute does not define "communication" and no Massachusetts decision expounds on its meaning. Webster's Third New International Dictionary first defines "communication" as "the act or action of imparting or transmitting <the ~ of the common cold> <the ~ of power to the machine>."[6] Webster's Third New International Dictionary at 460 (2002). See Commonwealth v. Moody, 466 Mass. 196, 208-209 (2013) (because "record" not defined in Wiretap Statute, court looked to "common and approved usage," including Webster's Third New International Dictionary). Given this definition, the term as used in the Wiretap Statute may fairly be interpreted to encompass the website interactions captured by SRC. The mouse movements, clicks, keystrokes, and other browsing activity that SRC records plausibly constitute an exchange of information between the website's owner and the website user. See, e.g., Hammerling v. Google LLC, 615 F. Supp. 3d 1069, 1092 (N.D. Cal. 2022) ("Although there is

[6] Accord State v. Ozuna, 184 Wash. 2d 238, 247 (2015) ("communication" is "the act or action of imparting or transmitting" or the "interchange of thoughts or opinions: a process by which meanings are exchanged between individuals through a common system of symbols (as language, signs, or gestures)"), quoting Webster's Third New International Dictionary 460 (2002); Regents of Univ. of Minnesota v. AGA Med. Corp., No. 07-CV-4732 PJS/LIB, 2011 WL 13943 at * 3 n.4 (D. Minn. Jan. 4, 2011); Rafferty v. NYNEX Corp., No. CIV.A.87-1521HHG/PJA, 1989 WL 38946 at * 1 (D.D.C. Apr. 4, 1989).

some oddity in construing the collection of data related to app usage as involving 'communications,' it is at least plausible that it does."); Revitch v. New Moosejaw, LLC, No. 18-CV-06827-VC, 2019 WL 5485330 at *1 (N.D. Cal. Oct. 23, 2019) ("[A] customer who calls to inquire about a store's products undoubtedly communicates with the retailer. As does an online patron. Revitch requested information from Moosejaw by clicking on items of interest; Moosejaw responded by supplying that information. This series of requests and responses – whether online or over the phone – is communication.").

Defendant's argument that an Internet-based interaction does not occur by using wire, cable, or another like connection, disregards plaintiff's allegations, see, e.g., Complaint ¶¶ 24 ("website delivers [SRC] to a user's browser"), 25 ("Events are typically accumulated and transmitted in blocks periodically throughout the user's website session"), 49 (SRC provides "instantaneous transmissions to the [SRP]"), 70, 76, and overlooks the fact that the mechanism for Internet interactions is the result of technology rooted in telephone infrastructure. Cf. United States v. Lyons, 740 F.3d 702, 716 (1st Cir. 2014) ("the internet is an 'instrumentalit[y] . . . used or useful in the transmission of writings, signs, pictures, and sounds of all kinds by aid of wire, cable, or other like connection between the points of origin and reception of such transmission.'"), quoting 18 U.S.C. § 1081. Moreover, the Supreme Judicial Court has not narrowly construed the phrase "wire communication." See Moody, 466 Mass. at 208 (definition of "wire communication" in Wiretap Statute is "broad[ ]" and encompasses "non-oral electronic transmissions"). Thus, although there appears to be no Massachusetts authority directly on point, Internet-based interactions plausibly involve the use of cable or wire or, at the very least, a

connection "like" cable or wire.[7] BJ's is not entitled to dismissal of Count I for failure plausibly to allege that the SRC affected a wire communication.[8]

B. Interception

In relevant part, under the Wiretap Statute, "'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) (emphasis added). BJ's contends that, even if plaintiff's interaction with its website constituted wire communications, plaintiff has failed to allege an "interception" because it has failed to allege (i) that the contents of any wire communication were recorded during his visits to its website, or (ii) that SRC is an intercepting device. These arguments are also unavailing.

1. Contents

The term "contents," as used in the definition of "interception," "means any information concerning the identity of the parties to [any wire or oral] communication or the existence,

---

[7] BJ's relies on Mastel v. Miniclip SA, 549 F. Supp. 3d 1129, 1134-1136 (E.D. Cal. 2021), which analyzed a claim brought under the first clause of Cal. Penal Code § 631(a). Unlike the Massachusetts Wiretap Statute, § 631(a) applies only to the tapping of a "telegraph or telephone wire, line, cable, or instrument." (Emphasis added). Mastel, 549 F. Supp. 3d at 1134-1136. The case is inapposite in the context of the Massachusetts Wiretap Statute's broader language.

[8] Citing to "the point of origin and the point of reception" language in the definition of "wire communication" and Ninth Circuit case law, BJ's also argues that plaintiff has not alleged an actionable wire communication because he admits that SRC intercepts contents only after it is received. See Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876-879 (9th Cir. 2002) (for website to be "intercepted" in violation of the federal wiretap act it must be acquired during transmission, not while it is in electronic storage). Even assuming the Massachusetts Wiretap Statute contains a real-time interception requirement, I do not read the Complaint as making such an admission. See Complaint, ¶¶ 1, 24, 78. See also In re Pharmatrak, Inc., 329 F.3d 9, 21 (1st Cir. 2003) (declining to adopt or reject real time requirement, but stating "the storage-transit dichotomy adopted by earlier courts may be less than apt to address current problems").

contents, substance, purport, or meaning of that communication." Id. at § 99(B)(5). Defendant argues that SRC does not capture "content," but simply records the actions of a website visitor. Given the breadth of the statutory definition, the Complaint plausibly suggests that keystrokes, clicks, mouse movements, URLs, and other data allegedly recorded by SRC constitute contents. See Commonwealth v. Mejia, 64 Mass. App. Ct. 238, 243 (2005) ("'Contents' . . . is defined broadly"), quoting District Attorney for Plymouth Dist. v. New England Tel. & Tel. Co., 379 Mass. 586, 591-592 (1980).

The authorities that BJ's cites are not persuasive. To argue that its SRC did not record "contents," BJ's points to Commonwealth v. Hyde, 434 Mass. 594, 605 n.11 (2001), and Commonwealth v. Camilli, 81 Mass. App. Ct. 1129, 2012 WL 1284387 at * 2 n.4 (Apr. 17, 2012) (Rule 1:28 decision). Both decisions held that silent video recordings did not implicate the Wiretap Statute because they did not intercept "oral communications" under the statute. Although BJ's argues that SRC is analogous to a surveillance camera that does not record audio, here we are dealing with "wire communications," which were not at issue in either case.

Defendant also cites several decisions from Florida and California that address whether SRC and other software violated Florida, California, and/or federal wiretap statutes. See, e.g., Jacome v. Spirit Airlines Inc., No. 2021-000947-CA-OI, 2021 WL 3087860 at * 4 (Fla. Cir. Ct. June 17, 2021) (no content intercepted under Florida statute); Brodsky v. Apple Inc., 445 F. Supp. 3d 110, 127 (N.D. Cal. 2020) (under federal and California statutes "user names, passwords, and geographic location information are not contents"). However, all three statutes define "contents" much more narrowly than G.L c. 272, § 99(B)(5), as any "information concerning the substance, purport, or meaning of [any wire, oral, or electronic] communication." 18 U.S.C. § 2510(8); Fla. Stat. § 934.02(7); Brodsky, 445 F. Supp. 3d at 127 (Cal. Penal Code §

631(a) incorporates definition in 18 U.S.C. § 2510(8)). In contrast, the Massachusetts statute defines "contents" also to include "information concerning the identity of the parties" or "the existence . . . of that communication."[9] Accordingly, the Florida and California cases have little persuasive value. See In re Zynga Privacy Litig., 750 F.3d 1098, 1106 (9th Cir. 2014) ("the term 'contents' under the federal wiretap statute refers to the communication's intended message and not record information regarding the characteristics of the message from the fact that the definition of contents was amended in 1986 to remove the phrase "identity of the parties to such communication").[10] Plaintiff has sufficiently alleged that the SRC on defendant's website recorded the "contents" of a wire communication under the Massachusetts Wiretap Statute.

2. Intercepting Device

BJ's also argues that SRC is not an intercepting device. The Massachusetts Wiretap Statute defines an intercepting device, in relevant part, as:

> 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 . . . "

G.L. c. 272, § 99(B)(3) (emphasis added). BJ's asserts that SRC is not a device or apparatus, or falls within the clause that begins "other than," which is referred to as the telephone equipment exception. Neither contention is availing.

---

[9] The Massachusetts statute also circularly defines "contents" to include "any information concerning . . . the . . . contents . . . of that [wire] communication." G.L. c. 272, § 99(B)(4).

[10] Both Florida and California courts look to In re Zynga Privacy Litigation to determine if "contents" have been intercepted. See, e.g., Jacome, 2021 WL 3087860 at * 3; Brodsky, 445 F. Supp. 3d at 127.

In support of its first argument, defendant relies entirely on In re Facebook Internet Tracking Litig., a decision in which a federal district court in California dismissed a lawsuit alleging that Facebook violated the California wiretap statute by embedding cookies in plaintiffs' internet browsers. 140 F. Supp. 3d 922, 925, 937 (N.D. Cal. 2015). The court found the plaintiff's complaint failed to state a claim because it "only define[d] a cookie as a small text file containing a limited amount of information which sits idly on a user's computer until contacted by a server." Id. at 937. Because the facts here are different, the decision is inapposite. SRC is significantly different from the cookies at issue in that case; SRC allegedly captures an individual's data in a manner that is much more active and invasive. Several other decisions have suggested that SRC may be an intercepting device. See Rich v. Rich, No. BRCV200701538, 2011 WL 3672059 at *6 (Mass. Super. July 8, 2011) (McGuire, J.), quoting G.L. c. 272, § 99(B)(3) (key logger program was "an 'intercepting device' (at least when surreptitiously installed on a computer) because it 'is capable of . . . recording a wire . . . communication'"); Makkinje v. Extra Space Storage, Inc., No. 8:21-CV-2234-WFJ-SPF, 2022 WL 80437 at *2 (M.D. Fla. Jan. 7, 2022) (software may constitute a device in wiretapping context); United States v. Hutchins, 361 F. Supp. 3d 779, 795 (E.D. Wis. 2019) ("The majority of courts to consider this issue have entertained the notion that software may be considered a device for the purposes of the [Federal] Wiretap Act.").

With regard to its second contention, BJ's cites Dillon v. Massachusetts Bay Transp. Auth., 49 Mass. App. Ct. 309 (2000), as suggesting the SRC that it deploys, which it obtained from third-party SRPs, falls under the telephone equipment exception, i.e. the equivalent of "telephone . . . equipment . . . furnished to a subscriber or user by a communications common carrier [i.e., a telephone company] in the ordinary course of its business." In Dillon, the court

held that recording machines were covered by the exception even though they were furnished by non-telephone company sources. 49 Mass. App. Ct. at 314-316. In so ruling, it explained:

> We do not depart lightly from the express wording of a statute, but in the unusual circumstances appearing here . . . a deviation is justified. The fact that there has been no amendment of the Massachusetts statute . . . does not bar us from reading the exception so as to preserve it in its intrinsic intended scope and maintain its viability in the broad run of cases; the plaintiffs' proposal would in effect destroy the exception. Thus the decision below comports with the canons that interpretation should tend to preserve the substance of a statute rather than diminish it; should not override common sense; or produce absurd or unreasonable results — in this case the absurdity of allowing the fortuity of the source of the equipment to entail serious material consequences.

Id. at 315–316 (internal citations and footnote omitted). This analysis offers little guidance as to whether our appellate courts would depart even more dramatically from the language of G.L. c. 272, § 99(B)(3), and expand the exception to include software such as SRC, which has characteristics quite different from telephone equipment. Without such guidance, I decline to deviate so substantially from the statute's plain language.[11]

III. Invasion of Privacy Claim

Plaintiff asserts that use of SRC is an invasion of privacy under G.L. c. 214, § 1B ("A person shall have a right against unreasonable, substantial or serious interference with his privacy. The superior court shall have jurisdiction in equity to enforce such right and in connection therewith to award damages."). A claim of violation of Section 1B may be either

[11] BJ's contends that it used SRC in the ordinary course of business, a phrase which "translates as legitimate business purpose." Dillon, 49 Mass. App. Ct. at 319 (internal quotes omitted). Even assuming SRC could be considered telephone equipment, whether this is true would be a question of fact not properly resolved on a motion to dismiss. Cf. Marquis v. Google, Inc., No. 11-2808, 2012 WL 12929513 at * 4 (Mass. Super. Jan. 17, 2012) (Lauriat, J.) ("At this preliminary stage, the court cannot conclude as a matter of law that intercepting and scanning emails for purposes of 'interest-based advertising' is 'in the ordinary course of [Google's] business' under the Massachusetts wiretap statute.").

based on public disclosure of private facts or intrusion upon the plaintiff's solitude or seclusion, i.e., an infringement upon the right to be left alone. Polay v. McMahon, 468 Mass. 379, 382 (2014). In either case, the plaintiff must plausibly allege that the invasion was both unreasonable and substantial or serious. Id.

At the hearing, plaintiff clarified that his claim is based on an intrusion upon his solitude or seclusion, rather than the disclosure of private facts. See also Complaint ¶ 90. "Factors . . . considered in assessing whether there has been an intrusion that is unreasonable, as well as substantial or serious, include the location of the intrusion, the means used, the frequency and duration of the intrusion, and the underlying purpose behind the intrusion." Polay, 468 Mass. at 383. The court must "balance the extent to which the defendant violated the plaintiff's privacy interests against any legitimate purpose the defendant may have had for the intrusion." Id. Typically, whether an intrusion is unreasonable, substantial, or serious is a fact question. Id. [12]

Plaintiff contends he has alleged an intrusion on his solitude or seclusion by alleging that each time he visited defendant's website on his smartphone or computer, the SRC secretly collected his personal data in real-time for defendant's monetary gain without his consent. I am somewhat skeptical that these allegations are sufficient to state a claim for invasion of privacy. Among other things, plaintiff has failed to allege clearly that BJ's was able to connect his identity to the data collected or that the data collected was particularly personal or sensitive. The Complaint merely alleges that plaintiff went to defendant's website to shop for tires, an activity

[12] In Polay, the Court explained that "[m]ost of our jurisprudence under th[e] statute has involved public disclosure of private facts[.]" 468 Mass. at 382, citing Ayash v. Dana-Farber Cancer Inst., 443 Mass. 367, 382 n.16, cert. denied sub nom Globe Newspaper Co., Inc. v. Ayash, 546 U.S. 927 (2005). In such cases, "[t]he statute, essentially, proscribes 'disclosure of facts about an individual that are of a highly personal or intimate nature when there exists no legitimate countervailing interest.'" Ayash, 443 Mass. at 383, quoting Bratt v. International Business Mach. Corp., 392 Mass. 508, 518 (1984).

unlikely to reveal information that is either particularly personal or of durational relevance. Cf. In re Facebook, Inc. Internet Tracking Litig., 956 F.3d 589, 604 n.7 (9th Cir. 2020) ("individuals have a reasonable expectation of privacy in collections of information that reveal familiar, political, professional, religious, and sexual associations") (internal quotes omitted), cert. denied, 141 S Ct. 1684 (2021); McLaughlin v. Meehan, No. 1681CV00866, 2018 WL 1041371 at *10 (Mass. Super. Jan. 19, 2018) (Tuttman, J.) (plaintiff stated claim where defendants searched his computer files, including email accounts, containing his "thoughts, ideas, and communications").

Nevertheless, for three reasons I am hesitant at this early stage to conclude as a matter of law that the SRC on defendant's website did not cause the type of intrusion covered by the statute. First, the question of whether an intrusion transgresses the privacy statute is a fact question. Second, as suggested by some of the statistics cited in the Complaint, what constitutes acceptable data collection on the Internet appears to be evolving. See, e.g., Polay, 468 Mass. at 383 ("[T]he Legislature appears to have framed the statute in broad terms so that the courts can develop the law thereunder on a case-by-case basis, by balancing relevant factors . . . and by considering prevailing societal values and the ability to enter orders which are practical and capable of reasonable enforcement."), quoting Schlesinger v. Merrill Lynch, Pierce, Fenner & Smith, Inc., 409 Mass. 514, 519 (1991). Third, plaintiff's claim under the Wiretap Statute will proceed to discovery and the scope of discovery will not differ if plaintiff's claim under G.L. c. 214, § 1B remains.[13]

[13] BJ's also argues plaintiff's privacy claim fails because its interest in collecting plaintiff's data does not outweigh his privacy interest. This is a question of fact not appropriate for resolution on a motion to dismiss. See Polay, 468 Mass. at 384 ("Whether McMahon acted for the legitimate purpose . . . that outweighs any incidental intrusion on the plaintiffs' privacy . . . is . . . a question of fact not suitable for resolution on a motion to dismiss.").

BJ's also argues with limited analysis that plaintiff may only look to the Wiretap Statute for relief because G.L. c. 272, § 99(Q), provides an exclusive civil remedy for those "whose personal or property interests or privacy were violated by means of an interception" and the invasion of privacy claim is based on the same facts.[14] In support, defendant cites two trial court decisions: Christensen v. Cox, No. SUCV201701635BLS1, 2017 WL 7053911 at * 7 (Mass. Super. Nov. 21, 2017) (Leibensperger, J.), and Tedeschi v. Reardon, 5 F. Supp. 2d 40, 46 (D. Mass. 1998) (Stearns, J.). In both cases, the trial court concluded that the Wiretap Statute is the exclusive remedy when conversations are illegally intercepted. Neither decision, however, offers much reasoning to support its conclusion. Christensen merely cites to Tedeschi and Tedeschi merely cites to G.L. c. 272, § 99(Q) and Charland v. Muzi Motors, Inc., 417 Mass. 580, 585-586 (1994), which held that G.L. c. 151B provides the exclusive remedy for employment discrimination not based on pre-existing tort law or constitutional protections. Charland was based, at least in part, on the existence of an exclusivity provision in G.L. c. 151B. 417 Mass. at 584-585. The Wiretap Statute does not have a comparable exclusivity provision. Thus, it is unclear whether the Legislature intended the two remedies to co-exist in the situation before me. While defendant's argument may ultimately have merit, without more comprehensive analysis from the parties, I am reluctant to decide the issue on a motion to dismiss for the same reasons discussed above – dismissal will not change the overall scope of the case.[15]

---

[14] The Wiretap Statute was enacted in substantially its present form in 1968, before the enactment of G.L. c. 214, § 1B.

[15] At the hearing, plaintiff suggested that his privacy claim was based not on an interception occasioned by the SRC but on BJ's "embedding" code on his browser. Even setting aside that this was not clearly pled in the Complaint or argued in plaintiff's opposition, such a claim would necessarily fail. It is difficult to understand how merely installing SRC, as opposed to (or without) its active use, results in any invasion of privacy. Cf. Polay, 468 Mass. at 381-385

ORDER

Defendant's Motion to Dismiss (Docket #12) is **DENIED**.

Dated: June 21, 2023

_____
Peter B. Krupp
Justice of the Superior Court

(plaintiff stated claim for invasion of privacy where plaintiff alleged defendant's cameras *recorded* plaintiffs' house).