IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

DAKOTAH MASSIE and NEIL MANGLANI, individually and by and on behalf of all others similarly situated,

Plaintiffs,

v.

GENERAL MOTORS LLC and DECIBEL INSIGHT, INC.,

Defendants.

Civil Action No. 21-787-RGA

MEMORANDUM OPINION

Blake A. Bennett, Dean R. Roland, COOCH AND TAYLOR, Wilmington, DE; Max S. Roberts, BURSOR & FISHER, P.A., New York, NY.

Attorneys for Plaintiffs.

Oderah C. Nwaeze, FAEGRE DRINKER BIDDLE, Wilmington, DE; Benjamin J. Schladweiler, GREENBERG TRAURIG, LLP, Wilmington, DE; John Nadolenco, MAYER BROWN LLP, Los Angeles, CA; Archis A. Parasharami, MAYER BROWN LLP, Washington, D.C.; Ian C. Ballon, GREENBERG TRAURIG, LLP, Los Angeles, CA; Justin A. MacLean, GREENBERG TRAURIG, New York, NY.

Attorneys for Defendants.

February 17, 2022

ANDREWS, UNITED STATES DISTRICT JUDGE:

Before me are two motions to dismiss under Rule 12(b)(1) for lack of subject matter jurisdiction and under Rule 12(b)(6) for failure to state a claim. (D.I. 50, 53). The motions have been fully briefed and I have considered the parties' briefing. (D.I. 51, 54, 56, 57, 58).

I. BACKGROUND

Plaintiffs Dakotah Massie and Neil Manglani bring this class action suit against Defendants GM and Decibel. They allege four Counts, all based on GM's use of Decibel's "Session Replay" software on GM's websites. Counts I and II claim violations of Sections 631 and 635 of the California Invasion of Privacy Act (CIPA) by both Defendants; Count IV claims a violation of Section 2512 of the Federal Wiretap Act by Decibel; and Count III claims an invasion of privacy under California's Constitution. Plaintiffs withdrew Count III in the briefing. (D.I. 56 at 25 n.13).

Plaintiffs seek to represent a class of "all residents in the United States who visited [websites owned and operated by GM ("the Website")], and whose electronic communications were intercepted or recorded by Decibel" and a subclass of "all California residents who visited the Website, and whose electronic communications were intercepted or recorded by QM (sic)[1]." (D.I. 25 ¶¶ 50, 51). Both classes are asserted in Count IV; only the California class is asserted in Counts I and II. One of the consequences of the oddities of personal jurisdiction is that this case, which was originally filed in California, was transferred to Delaware. (D.I. 38). There is no basis for the federal claim,[2] so this case in Delaware boils down to two Californians seeking to represent a class limited to Californians asserting only violations of California law.

---

[1] I think QM is a cut-and-paste remnant from a separate lawsuit against Quantum Metrics. I think Plaintiffs mean Decibel, not QM.

[2] The California District Courts may disagree about the merits of some of the California claims, but they appear to agree that no federal wiretapping claim is stated. *See Yoon v. Lululemon*

Section 631 of the CIPA applies to:

> any person who, by means of any machine, instrument, or contrivance, or in any other manner, intentionally taps, or makes any unauthorized connection… with any … communication system, or who willfully and without the consent of the parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state.

Section 635 of the CIPA applies to:

> Every person who manufactures, assembles, sells, offers for sale, advertises for sale, possesses, transports, imports, or furnishes to another any device which is primarily or exclusively designed or intended for eavesdropping upon the communication of another, or any device which is primarily or exclusively designed or intended for the unauthorized interception or reception of communications between cellular radio telephones…

Section 2512 of the Federal Wiretap Act applies to any person who intentionally:

> manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce.

18 U.S.C. § 2512(1)(b).

Decibel's Session Replay software records website users' mouse movements, clicks, and keystrokes, producing "video-accurate renders of real visits" to websites. (D.I. 25 ¶¶ 23, 26). The software also captures the date, time, and duration of a user's visit, as well as the user's IP address, "location at the time of the visit[]," browser type, and device's operating system. (*Id.* ¶ 41). GM uses Decibel's Session Replay software on its websites. (*Id.* ¶ 35).

USA, Inc., 2021 WL 3615907, at *7-8 (C.D. Cal. July 15, 2021) (§2512); *Mastel v. Miniclip SA*, 2021 WL 2983198, at *10-11 (E.D. Cal. July 15, 2021) (§2701).

Massie and Manglani visited one of GM's websites, Chevrolet.com, in August and September of 2020 on a combined three occasions. (*Id.* ¶¶ 39, 40). On those visits, Massie and Manglani "browsed the vehicle sections" but did not purchase anything and, therefore, did not input any of their personal information (*e.g.*, name, zip code, phone number, email address). (*Id.* ¶¶ 39, 40, 43, 44).

II. DISCUSSION

Because Article III standing is a prerequisite for a federal court's subject matter jurisdiction, a motion to dismiss for lack of standing is properly brought under Fed. R. Civ. P. 12(b)(1). *Ballentine v. United States*, 486 F.3d 806, 810 (3d Cir. 2007). To establish standing under Article III, a plaintiff must have "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision." *Spokeo, Inc. v. Robins*, 578 U.S. 330, 338 (2016). "The plaintiff, as the party invoking federal jurisdiction, bears the burden of establishing these elements." *Id.* "To establish an injury in fact, a plaintiff must show that he or she suffered an invasion of a legally protected interest that is concrete and particularized and actual or imminent, not conjectural or hypothetical." *Id.* at 339. "That a suit may be a class action adds nothing to the question of standing, for even named plaintiffs who represent a class must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong." *Id.* at 338 n.6 (cleaned up).

"Article III standing requires a concrete injury even in the context of a statutory violation." *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2205 (2021).[3] The "Court has rejected the

[3] There is only one precedential Third Circuit opinion to date that cites *TransUnion*, and that opinion does not add any gloss that is helpful on the issue here.

proposition that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right." *Id.* (cleaned up). "[A]n injury in law is not an injury in fact. Only those plaintiffs who have been *concretely harmed* by a defendant's statutory violation may sue that private defendant over that violation in federal court." *Id.* While "traditional tangible harms, such as physical harms and monetary harms" are "obvious[ly]" concrete, "[v]arious intangible harms can also be concrete." *Id.* at 2204. "Chief among them are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts. Those include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion." *Id.* (cleaned up).

In *TransUnion*, where the plaintiffs sought to sue a credit reporting agency for preparing credit reports containing inaccurate information about the plaintiffs, the Court analogized the plaintiffs' injury to the common law tort of defamation. *TransUnion*, 141 S. Ct. at 2208. The Court found that the plaintiffs whose inaccurate credit reports had not been provided to any potential creditors had not suffered a concrete injury, because a critical element of defamation – dissemination – was lacking. *Id.* at 2209-10 ("The mere presence of an inaccuracy in an internal credit file, if it is not disclosed to a third party, causes no concrete harm."). The Court also found that the risk of future harm to the plaintiffs by the potential disclosure of their incorrect credit reports in the future was insufficient to qualify as a concrete harm. *Id.* at 2210-12 ("[P]laintiffs' argument for standing for their damages claims based on an asserted risk of future harm is unavailing.").

Here, Plaintiffs analogize their injury to an invasion of privacy or a harm to their "interest in controlling their personal information." (D.I. 56 at 7-8). "[B]oth the common law and the literal

understandings of privacy encompass the individual's control of information concerning his or her person." *U.S. Dept. of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 763-64 (1989). Plaintiffs cite a slew of cases in which courts have recognized invasion of privacy as an injury sufficient to confer standing. (D.I. 56 at 7-8). I find, however, that the critical facts of the cases Plaintiffs cite concerning an invasion of privacy injury are distinguishable from the facts at issue here. Each of Plaintiffs' cited cases involves the collection and disclosure of personal information. Here, Plaintiffs do not allege that any of their information collected by the Session Replay software was personal or private within the common law understanding of a privacy right. Therefore, I find Plaintiffs have not suffered a concrete injury because they do not have a privacy interest at stake.

I now review the cases upon which Plaintiffs rely and explain why they do not help Plaintiffs.

In *In re Facebook*, Facebook used "plug-ins to track users' browsing histories when they visit[ed] third-party websites, and then compile[d] these browsing histories into personal profiles which [were] sold to advertisers to generate revenue." *In re Facebook, Inc. Internet Tracking Litig.*, 956 F.3d 589, 596 (9th Cir. 2020). Facebook continued to track users' browsing even after they had logged out of Facebook. *Id.* The Court found that this behavior amounted to a concrete and particularized injury, as it caused "harm or a material risk of harm to [plaintiffs'] interest in controlling their personal information." *Id.* at 599. In reaching this conclusion, the Court emphasized the comprehensive nature of the tracking, and how it allowed Facebook to piece together a "cradle-to-grave profile without users' consent" by "correlating users' browsing history with users' personal Facebook profiles." *Id.* at 598-99 ("[T]his tracking occurred 'no matter how sensitive' or personal users' browsing histories were"). The degree of the invasion of privacy at

issue in *In re Facebook* is hardly comparable to the "invasion of privacy" Plaintiffs allege here. GM only recorded Plaintiffs' browsing while Plaintiffs were on GM's own website, GM obtained no personal information from Plaintiffs, and Plaintiffs make no allegations that GM attempted to sell or monetize the information it collected in any way

In *In re Nickelodeon*, the plaintiffs alleged that Viacom tracked children's "web browsing and video-watching habits on Viacom's websites" and then used that browsing information, in addition to user account information including the child's username/alias, gender, and birthdate, "to sell targeted advertising based on users' web browsing." *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 269 (3d Cir. 2016). The Court specifically pinpointed "the unlawful disclosure of legally protected information" as the concrete harm giving rise to Article III standing. *Id.* at 274. Here, Plaintiffs have not provided a basis for the conclusion that the information GM collected was "legally protected," nor have they alleged any "unlawful disclosure" of such information.

In *In re Google*, the Court found the plaintiffs had been injured based "on highly specific allegations that the defendants, in the course of serving advertisements to their *personal* web browsers, implanted tracking cookies on their *personal* computers." *In re Google Inc. Cookie Placement Consumer Privacy Litigation*, 806 F.3d 125, 134 (3d Cir. 2015). Unlike here, where Plaintiffs' browsing activities were only recorded while Plaintiffs were visiting GM's website, in *In re Google*, the defendants circumvented users' "cookie blockers" settings to "compile the internet histories of users," "create detailed profiles on individuals," and then serve targeted ads to users based on that activity. *Id.* at 131. Such conduct is far more invasive than the conduct alleged here.

In *Eichenberger*, the Court found that the plaintiff sustained a concrete injury when "Defendant knowingly disclosed to a third party, AdobeAnalytics: (1) Plaintiff's Roku device serial number and (2) the identity of the video that he watched." *Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 981 (9th Cir. 2017). Adobe then used that information "to identify specific consumers by connecting that information 'with existing data already in Adobe's profile of those individuals'" such as "'email addresses, account information, or Facebook profile information, including photos and usernames.'" *Id.* Adobe then gave the resulting data back to the defendant, who in turn "provide[d] advertisers with aggregated information about its users' demographics." *Id.* The Court predicated its finding that plaintiff had suffered a concrete injury on its conclusion that a person's "*substantive* right to privacy [] suffers *any time* a video service provider discloses otherwise private information." *Id.* at 983-84. Here, Plaintiffs have not alleged any disclosure of any of their private information. Insofar as Plaintiffs have alleged GM disclosed their non-private information to Decibel,[4] they have not alleged that Decibel used that information in any way, let alone in a way that harmed or would likely harm Plaintiffs.

In *Moosejaw*, the Court found the plaintiff had suffered a concrete injury where the defendant "helped [a third party] eavesdrop on [plaintiff's] communications and scan [plaintiff's]

---

[4] The only statements Plaintiffs make in their First Amended Complaint ("FAC") that allege Decibel received any of the information GM collected are found in the "The Parties" section of the FAC. There, Plaintiffs state, Plaintiffs' "keystrokes, mouse clicks, and other electronic communications were intercepted in real time and were disclosed to Defendants GM and Decibel through the wiretap," and each Plaintiff was "unaware at the time that his keystrokes, mouse clicks and other electronic communications were being intercepted in real-time and would be disclosed to Decibel, nor did [each Plaintiff] consent to the same." (D.I. 25 ¶¶ 4-5).

Plaintiffs do not, however, make any specific allegations in the FAC's "Statement of Facts" section to support these conclusory allegations. The allegations in the Statement of Facts section suggest GM merely used Decibel's software. They do not specifically allege that Decibel received any of the information collected by GM, in real time or otherwise.

computer for files revealing his identity." *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330, at *1 (N.D. Cal. Oct. 23, 2019). The Court reasoned, "Being eavesdropped upon is a concrete (though intangible) harm, as is having one's computer files surreptitiously scanned." *Id.*

Moosejaw does not help Plaintiffs. As explained in note 4, *supra*, I am unconvinced that Plaintiffs here have specifically alleged activity by Decibel that amounts to eavesdropping. Nevertheless, even if Plaintiffs have alleged that anonymous information about their browsing activities on GM's website was shared with Decibel, I do not think it follows that the reasoning of *Moosejaw* about being "eavesdropped" applies. Whether there is a concrete harm depends on the nature of the allegations; to say otherwise would be at odds with the Supreme Court's clarification of standing doctrine in *TransUnion*. A legislature's "creation of a statutory prohibition or obligation and a cause of action does not relieve courts of their responsibility to independently decide whether a plaintiff has suffered a concrete harm under Article III." *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190, 2205 (2021). "Only those plaintiffs who have been *concretely harmed* by a defendant's statutory violation may sue that private defendant over that violation in federal court." *Id.*

Just as a claim for defamation requires disclosure of defamatory information, a claim of invasion of privacy requires an intrusion upon something over which a person has a reasonable expectation of privacy. "Eavesdropping" on communications that do not involve personal information, personally identifiable information, or information over which a party has a reasonable expectation of privacy does not amount to a concrete injury. Plaintiffs do not have a reasonable expectation of privacy over the anonymized data captured by the Session Replay software at issue here.

Plaintiffs argue that the injury they have suffered is rooted in their "interest in controlling their personal information." (D.I. 56 at 8). I agree that Plaintiffs have a legally cognizable interest in controlling their personal information and that intrusion upon that interest would amount to a concrete injury. The fact of the matter remains, however, that none of Plaintiffs' personal information is implicated by the allegations they make. Plaintiffs fail to explain how either GM's or Decibel's possession of anonymized, non-personal data regarding their browsing activities on GM's website harms their privacy interests in any way.

Finally, in *Mastel*, the only post-*TransUnion* case cited by Plaintiffs on the issue of standing, the District Court found "allegations that a company has violated a plaintiff's right to privacy ... by collecting personal information without the plaintiff's consent involve a sufficiently 'concrete' injury, even if there are no additional allegations of publication, because the invasion itself causes harm to the plaintiff's interest in controlling the information." *Mastel v. Miniclip SA*, 2021 WL 2983198, at *6 (E.D. Cal. July 15, 2021). The facts in *Mastel*, however, are readily distinguishable from those at issue here. *Mastel* involved a mobile application that was able to "view, copy, and save" whatever text the user had most recently "copied" on his mobile device any time the application was open. *Id.* at *1. The plaintiff alleged that some of the information the application had access to included "his name, email, phone number, and address, addresses of friends and relatives, and personal and private messages that have been sent to friends and relatives." *Id.* Here, Plaintiffs do not allege any collection of personal information of that nature.

"A material risk of future harm can satisfy the concrete-harm requirement" where a plaintiff "exposed to a risk of future harm" seeks "forward-looking, injunctive relief to prevent the harm from occurring," but the risk of harm must be "sufficiently imminent and substantial."

TransUnion, 141 S. Ct. at 2210. Plaintiffs have made no allegations suggesting a risk of future harm to them is imminent or substantial.

For these reasons, I will GRANT Defendants' motions to dismiss Counts I, II, and IV under Rule 12(b)(1) for lack of subject matter jurisdiction.[5] I will dismiss Count III as withdrawn.

---

[5] I do this with some hesitation. I am aware that, although a number of cases involving similar claims have been considered by other courts, my decision to dismiss Plaintiffs' claims for lack of subject matter jurisdiction is without an exact precedent. I attribute this to the fact that the precise question and facts before me now differ from those that were before those other courts.

In *Noom*, *Blue Nile*, and *Clicktale*, the Northern District of California dismissed nearly identical claims of wiretapping by providers of session replay software for failure to state a claim. *Graham v. Noom, Inc.*, 533 F.Supp.3d 823, 832 (N.D. Cal. 2021) (holding that because there were no allegations that the third party "intercepted and used the data itself," plaintiff did not plausibly plead third party software provider eavesdropped on plaintiffs' communications, but pled only that the third party was "a vendor that provides a software service"); *Johnson v. Blue Nile, Inc.*, 2021 WL 1312771 (N.D. Cal. Apr. 8, 2021) (similar); *Yale v. Clicktale, Inc.*, 2021 WL 1428400 (N.D. Cal. Apr. 15, 2021) (similar). In these cases, defendants argued (and the Court agreed) that, because plaintiffs failed to state a claim of eavesdropping under CIPA § 631(a), plaintiffs had suffered no injury and therefore lacked standing for their CIPA § 635(a) claim regarding the possession of a device "primarily or exclusively designed or intended for eavesdropping." *Noom*, 533 F.Supp.3d at 835; *Blue Nile*, 2021 WL 1312771, at *3; *Clicktale*, 2021 WL 1428400, at *3. Defendants did not, however, argue lack of subject matter jurisdiction over the CIPA § 631(a) "eavesdropping" claims.

In *Saleh*, *Yoon*, and *Alhadeff*, also involving session replay software, the Central District of California decided the Rule 12(b)(6) issue differently than did the Northern District of California cases. Defendants in *Yoon* and *Alhadeff* did not argue lack of subject matter jurisdiction at all, and defendant in *Saleh*, where plaintiff completed a purchase on defendant's website and thereby had his personal and payment information collected, did not argue lack of subject matter jurisdiction over the CIPA § 631(a) eavesdropping claim. *Saleh v. Nike, Inc.*, 2021 WL 4437734 (C.D. Cal. Sept. 27, 2021) (holding plaintiff failed to state a claim that website owner eavesdropped, plaintiff stated a claim that website owner aided in software provider's eavesdropping, and plaintiff had no standing for his CIPA § 635 claim because he did not allege any injury from defendant's mere possession of an eavesdropping device); *Yoon v. Lululemon USA, Inc.*, 2021 WL 3615907 (C.D. Cal. July 15, 2021) (holding plaintiff did not state a claim for violation of CIPA § 631(a)[ii] because she had not alleged third party intercepted "content," but did state a claim for violation of CIPA § 631(a)(iv) for aiding in wiretapping by "allow[ing] a third party to access the communication."); *Alhadeff v. Experian Info. Sol'ns., Inc.*, 2021 WL 3615834

III. CONCLUSION

For the reasons stated above, Defendants' motions to dismiss are GRANTED. Counts I, II, III, and IV are DISMISSED.

An appropriate order will issue.

(C.D. Cal. May 25, 2021) (holding defendant's own recording of plaintiff's part of the conversation was "sufficient to allege 'interception' [under Florida law]").

There are also Florida District Court cases addressing the same issues raised under Florida law, *see Makkinje v. Extra Space Storage, Inc.*, 2022 WL 80437 (M.D. Fla. Jan. 7, 2022) (denying motion to dismiss); *Goldstein v. Costco Wholesale Corp.*, 2021 WL 4134774 (S.D. Fla. Sept. 9, 2021) (granting motion to dismiss). Neither of these cases consider a motion to dismiss for lack of subject matter jurisdiction.

The only analogous cases I have seen where the question of concreteness was reached do not involve session replay software and are inapposite for reasons I have explained. In *Moosejaw*, the third party's embedded code was much more invasive than the session replay software at issue here, as it redirected the plaintiff's communications to a third party in real time and allowed the third party to "scan[] [plaintiff's] computer for files that revealed his identity and browsing habits." *Revitch v. New Moosejaw, LLC*, 2019 WL 5485330 (N.D. Cal. Oct. 23, 2019). In *Mastel*, where neither party contested the private nature of the information defendants collected, the Court's concreteness analysis focused on whether an invasion of privacy harm requires *disclosure* of private information and not, as is at issue here, whether an invasion of privacy harm requires the involvement of information that is private in the first place. *Mastel v. Miniclip SA*, 2021 WL 2983198 (E.D. Cal. July 15, 2021).