IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA

AMBER COOK, individually and on behalf of all others similarly situated, Plaintiff, v. GAMESTOP, INC., Defendant.	)	2:22-cv-1292

OPINION

This putative class action is the latest in a series of lawsuits filed across the country against online retailers over the alleged use of Session Replay Code. Session Replay Code allows website operators to record, save, and replay website visitors' interactions with a website, including "all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry, and numerous other forms of a user's navigation and interaction through a website." ECF 22, ¶ 25.

Plaintiff Amber Cook brings this latest installment on behalf of herself and those similarly situated after she allegedly browsed for products on Defendant GameStop, Inc.'s public website. She claims that GameStop used Session Replay Code to record her "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[.]" *Id.* ¶ 1. According to her, GameStop's conduct violates the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa.C.S. § 5701, *et seq.*, and constitutes the tort of intrusion upon seclusion. *Id.* ¶¶ 3, 82-111.

GameStop moves to dismiss Ms. Cook's amended complaint pursuant to Federal Rule of Civil Procedure 12(b)(1) for lack of subject matter jurisdiction and

pursuant to Federal Rule of Civil Procedure 12(b)(6) for failure to state a claim. ECF 25.

After careful consideration, the Court joins the increasing number of courts that have found that the type of conduct pled in Ms. Cook's amended complaint does not amount to a sufficiently concrete harm to confer standing and therefore will grant GameStop's motion under Rule 12(b)(1). But Ms. Cook's amended complaint would have a fundamental flaw even if she did have standing to pursue her claims. That's because she has failed to plead the necessary facts to support her claims for violation of the Wiretap Act or intrusion upon seclusion. That failure provides the Court with an alternative basis to dismiss the case under Rule 12(b)(6).

BACKGROUND

GameStop is an online and brick-and-mortar retailer for gaming consoles, games, and accessories. ECF 22, ¶ 42. GameStop operates the website www.gamestop.com, as well as its subpages. *Id.* GameStop procures and embeds various Session Replay Code from Session Replay Providers on its website to track and analyze website user interactions with www.gamestop.com and its subpages. *Id.* ¶ 43. One such Session Replay Provider with whom GameStop does business is Microsoft, which owns and operates a Session Replay Code called Clarity. *Id.* ¶ 45.

Session Replay Code allows website operators to record, save, and replay website visitors' interactions with a given website. *Id.* ¶ 22. Once the events have been recorded by a Session Replay Code, a website operator can view a visual reenactment of the user's visit through the Session Replay Provider, usually in the form of a video. *Id.* ¶ 27.

Ms. Cook visited www.gamestop.com and "browsed for different products for sale." *Id.* ¶ 58. While browsing, she used "her mouse to hover and click on certain products and typ[ed] search words into the search bar." *Id.* She also "selected a product to add to her shopping cart by clicking 'add to cart'," but ultimately did not

purchase anything. *Id.* She alleges that GameStop's Session Replay Code instantaneously captured her website browsing activities. *Id.* ¶ 59.

After Ms. Cook filed her original complaint, GameStop moved to dismiss her claims. ECF 11. In response, and with GameStop's consent, Ms. Cook filed an amended complaint to purportedly "address issues raised in [GameStop's First] Motion to Dismiss[.]" ECF 21. Not satisfied with that amendment, GameStop met and conferred with Ms. Cook a second time, as required by this Court's Practices and Procedures, "to determine whether the identified pleading deficiencies may be cured by amendment, and determined that they could not." ECF 26, p. 24. GameStop then filed the motion that is now before the Court. ECF 25. The Court held an oral argument on the motion on July 27, 2023. ECF 41.

DISCUSSION & ANALYSIS

I. Ms. Cook lacks standing to bring her claims.

GameStop argues that Ms. Cook lacks Article III standing to bring her claims in this case because she has not alleged that she suffered an injury in fact. The Court agrees.[1]

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.*

[1] A district court may treat a party's motion to dismiss for lack of subject-matter jurisdiction under Rule 12(b)(1) as either a facial or factual challenge to the court's jurisdiction. *Gould Elecs. Inc. v. United States*, 220 F.3d 169, 176 (3d Cir. 2000) (citation omitted). GameStop's Rule 12(b)(1) motion focuses on the allegations in Ms. Cook's complaint, and so the Court construes GameStop's motion as making a facial attack. "In reviewing a facial attack, the court must only consider the allegations of the complaint and documents referenced therein and attached thereto, in the light most favorable to the plaintiff." *Id.* (citation omitted).

The "first and foremost" element—an injury in fact—is the one at issue here. *Id.* (cleaned up). "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 (cleaned up). "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).

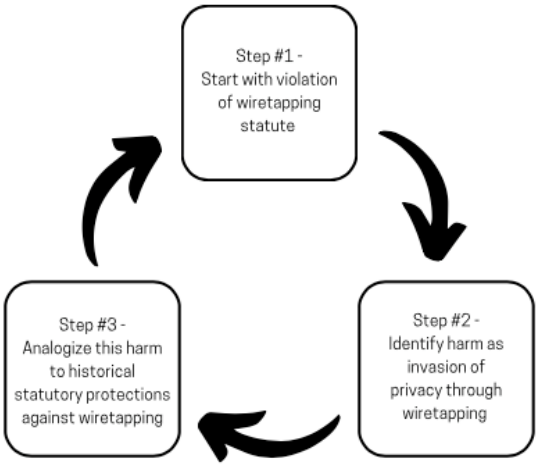
Even if a plaintiff alleges a statutory violation, like Ms. Cook does here, Article III standing still "requires a concrete injury[.]" *TransUnion LLC v. Ramirez*, 141 S.Ct. 2190, 2205 (2021) (cleaned up). As the Supreme Court explained in *TransUnion*, it is not enough that "a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right" because "an injury in law is not an injury in fact." *Id.* (cleaned up). Congress "may not simply enact an injury into existence, using its lawmaking power to transform something that is not remotely harmful into something that is." *Id.* (cleaned up). Rather, "[o]nly 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.* (emphasis in original). In other words, "for standing purposes," an "important difference exists between (i) a plaintiff's statutory cause of action to sue a defendant over the defendant's violation of federal law, and (ii) a plaintiff's suffering concrete harm because of the defendant's violation of federal law." *Id.*

There are "certain harms" that "readily qualify as concrete injuries under Article III." *Id.* at 2204. For example, "traditional tangible harms, such as physical harms and monetary harms" are "obvious[ly]" concrete. *Id.* Other, intangible harms are closer calls. These harms can be "concrete" if they bear "a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts."

Id. (citation omitted). "In looking to whether a plaintiff's asserted harm has a close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts, we do not require an exact duplicate." *Id.* at 2209 (cleaned up).

Here, Ms. Cook alleges that she has suffered the intangible harm of an "invasion of privacy," and analogizes that harm to "the age-old common law prohibitions and protections from and against invasion of privacy." ECF 43, 23:1-4. According to her, the Court need not analyze "the sensitivity of the information" that she alleges GameStop intercepted because there has been historical protection against "the idea of somebody eavesdropping on you, somebody intruding on your privacy, regardless of what the intrusion yields them." *Id.* at 56:20-57:5. Put simply, the mere fact that GameStop recorded ***any*** information about Ms. Cook's visit to GameStop's website is injury enough to give her standing to sue. But that circular reasoning simply folds back onto a bare statutory violation, which the Supreme Court has clarified cannot be the basis for standing.

Breaking down Ms. Cook's argument makes this point clear. Ms. Cook asks the Court to start its analysis with the violation of the wiretapping statute—that is, GameStop's alleged act of recording Ms. Cook's interactions with its website through the Session Replay Code. *Id.* at 25:10-14. After that, according to Ms. Cook, "the question then becomes do you have Article III harm because of that?" *Id.* at 25:15-16. Ms. Cook posits that, yes, you do, because "the act of the wiretap … intrudes upon your privacy." *Id.* at 25:16-22. And that harm is historically protected by wiretapping statutes, which means, in turn, that it is a traditionally recognized harm. *See id.* at 25:25-26:21 (analogizing Session Replay Code to wiretapping telephone lines). In other words, Ms. Cook is saying that the Court should analogize the harm under the wiretapping statute … to a violation of the wiretapping statute. Or something that looks like this:



Ms. Cook gave away the game when she pointedly argued that "the act of the wiretap … intrudes upon your privacy" and that's both the "injury under the statute" and the "analog to the injury under the tort." *Id.* at 25:15-24. Under Ms. Cook's argument, then, the Court's analysis should begin and end with the statutory violation.

Such an argument is no longer viable, however, because it runs directly counter to the Supreme Court's clarification that 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." *Lightoller v. Jetblue Airways Corp.*, No. 23-361, 2023 WL 3963823, at *3 (S.D. Cal. June 12, 2023) (citing *TransUnion*, 141 S. Ct. at 2205). To be sure, courts can no longer "treat an injury as concrete for Article III purposes based only on Congress's say-so." *TransUnion*, 141 S. Ct. at 2205 (cleaned up). To put a fine point on it: "a bare [statutory] violation by itself is insufficient to demonstrate Article III injury in fact." *Lightoller*, 2023 WL 3963823, at *3; *see also Byars v. Sterling Jewelers, Inc.*, No. 22-1456, 2023 WL 2996686, at *3 (C.D. Cal. Apr. 5., 2023) (rejecting the contention that "any violation of CIPA necessarily constitutes an injury in fact without the need for an additional showing of harm" because it conflicts with the holding in *TransUnion*); *Massie v. Gen. Motors LLC*, No. 21-787, 2022 WL 534468,

at *2, 5 (D. Del. Feb. 17, 2022) (dismissing statutory claims for lack of standing because plaintiff failed to allege a concrete injury).

So what does that mean for resolving GameStop's motion to dismiss? It means that the Court must examine the nature of the information that GameStop allegedly intercepted and determine whether the interception of that kind of information amounts to an invasion of privacy interests that have been historically protected. *See Massie*, 2022 WL 534468, at *4 ("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*."). "[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. Dep't of Justice v. Reporters Comm. For Freedom of Press*, 489 U.S. 749, 763 (1989) (emphasis added). This point is made clearer when one examines the two torts that Ms. Cook expressly mentions as being closely related to the conduct here: disclosure of private information and intrusion upon seclusion. ECF 31, pp. 5-12.

A claim for public disclosure of private information requires, obviously, "private facts" or information that the plaintiff does not leave "open to the public eye." Restatement (Second) of Torts § 652D cmt. b. A claim for intrusion upon seclusion requires a plaintiff to show that a defendant intentionally intruded "upon the solitude or seclusion of another or his private affairs or concerns," and that "the intrusion would be highly offensive to a reasonable person." *Popa v. Harriet Carter Gifts, Inc.*, 426 F. Supp. 3d 108, 120 (W.D. Pa. 2019) (Stickman, J.) (quoting Restatement (Second) of Torts § 625B). The requirement of private facts or private affairs in both torts confirms that the nature of the information is paramount. And "[e]avesdropping 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." *Massie*, 2022 WL 534468, at *5; *see*

also TransUnion, 141 S. Ct. at 2204 (concrete harm exists where alleged injury bears "a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts," such as "disclosure of private information" and "intrusion upon seclusion").

The information that GameStop allegedly intercepted does not clear this threshold. Ms. Cook alleges that GameStop intercepted data regarding her "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[.]" ECF 22, ¶ 1; *see also id.* ¶ 46. More specifically, Ms. Cook claims that during a visit to GameStop's website, she "browsed for different products for sale," "communicated with GameStop's website by using her mouse to hover and click on certain products and typing search words into the search bar[,]" and "selected a product to add to her shopping cart by clicking 'add to cart.'" *Id.* ¶ 58.

Perhaps more notable than what she allegedly did on GameStop's website is what she did ***not*** do. Ms. Cook did not enter any personally identifying information at any point during her interaction. Not her name. Not her address. Not her credit card information. Nothing that could connect her browsing activity to ***her***. She also doesn't allege that GameStop did anything to figure out who she was, either. In effect, everything Ms. Cook did on GameStop's website was completely anonymous. So, her allegations do not set forth a concrete harm.[2] *See, e.g.*, *Lightoller*, 2023 WL 3963823,

[2] That Ms. Cook's browsing activity here was anonymous is particularly significant and dooms any attempt to establish a concrete injury in fact. *Massie*, 2022 WL 534468, at *5 ("Plaintiffs do not have a reasonable expectation of privacy over the anonymized data captured by the Session Replay software at issue here."). That said, at least one court has found that no concrete injury exists even when a plaintiff provides very basic identifying information—like a name, address, and phone number—during the browsing session. *See, e.g.*, *I.C. v. Zynga, Inc.*, 600 F. Supp. 3d 1034, 1049-50 (N.D. Cal. 2022) (finding disclosure of "basic contact information, including one's email address, phone number, or … username" inadequate to establish Article III standing based on the "insufficient fit between the loss of

at *4 ("Although Plaintiff alleges that Defendant monitored and recorded her communications via software when she visited Defendant's website, Plaintiff does not allege that she disclosed any personal information when she visited the website. As such, no personal information was intercepted and recorded."); *Massie*, 2022 WL 534468, at *3 ("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.").

But even if Ms. Cook's browsing activity could have somehow been connected to her, it still wouldn't be enough. At most, the information that GameStop intercepted related to her product preferences. Product preference information is not personal information. This information is no different from what GameStop employees would have been able to observe if Ms. Cook had gone into a brick-and-mortar store and began browsing the inventory. Her physical movements in the store are like her mouse movements, her pauses to look at inventory are like her mouse pointer hovering over products, and her picking up video games off the shelf are like placing those same titles in her virtual cart. Ms. Cook certainly doesn't have a reasonable expectation of privacy in this kind of public shopping behavior in the physical world, and she doesn't have it in the digital world, either.

Ms. Cook's three main arguments in opposition do not move the needle. First, she relies on pre-*TransUnion* Third Circuit decisions in *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262 (3d Cir. 2016), and *In re Google Inc. Cookie Placement Cons.*

---

information alleged here and the common law privacy torts of … disclosure of private facts and intrusion upon seclusion."); *Brignola v. Home Properties, L.P.*, No. 10-3884, 2013 WL 1795336, at *12 (E.D. Pa. Apr. 26, 2013) ("The information alleged to be reported (and included in the exhibits) are Plaintiff's name, address, phone number, etc. These are not private facts actionable for an intrusion upon seclusion claim or publication of private life claim."). The Court need not address this issue because Ms. Cook didn't even provide her basic information when she browsed the GameStop website.

Priv. Litig., 934 F.3d 316 (3d Cir. 2019). A close look at those decisions reflects that they might be abrogated by *TransUnion*.[3] But even if they weren't, they are distinguishable.

In *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, together with user account information including the child's username/alias, gender, and birthdate, "to sell targeted advertising based on users' web browsing." 827 F.3d at 269. In *Google*, the plaintiffs similarly claimed that Google bypassed their cookie blockers and placed tracking cookies on their web browsers, thereby collecting private data about their personal internet browsing information. 934 F.3d at 321, 325. In both cases, the plaintiffs' ***personal*** information was captured—*i.e.*, registered account information in *Nickelodeon*, and tracking cookies embedded within the plaintiffs' personal computers and browsers in *Google*. In other words, the "private facts" disclosed included some form of personal information. As discussed above, Ms. Cook does not allege that GameStop captured any such personal information.

Second, Ms. Cook argues that the Court should not look to *Massie* for guidance because it is "an outlier" and "wrongly decided." ECF 31, p. 9. According to Ms. Cook, the court in *Massie* improperly "required the privacy interests the plaintiffs alleged *be identical* to the right to privacy recognized at common law." *Id.* at pp. 9-10

[3] In *Nickelodeon*, the Third Circuit reasoned that a concrete injury in fact existed because "Congress has long provided plaintiffs with the right to seek redress for unauthorized disclosures of information that, in Congress's judgment, ought to remain private." 827 F.3d at 274. And the Third Circuit in *Google* simply cited *Nickelodeon*. 934 F.3d at 325 ("The *Nickelodeon* decision … dictates that we recognize standing here."). Of course, the Supreme Court in *TransUnion*, as noted above, emphasized that courts can no longer "treat an injury as concrete for Article III purposes based only on Congress's say-so." *TransUnion*, 141 S. Ct. at 2205 (cleaned up). In *Nickelodeon* and *Google*, there is no analysis of any "close historical or common-law analogue for the[] asserted injury" apart from the statute. *Id.* at 2204.

(emphasis in original). The court in *Massie* did no such thing, however. Instead, the court there compared the conduct alleged to the analogous harms of invasion of privacy and an encroachment on the plaintiffs' "interest in controlling their personal information" and found that there was not a close relationship between the two. *Massie*, 2022 WL 534468, at *3-5. That is precisely what the Supreme Court instructed lower courts to do in *TransUnion*.

Third, Ms. Cook's citation to a recent post-*TransUnion* case as supplemental authority does not alter the analysis. ECF 44 (citing *Brown v. Google LLC*, No. 20-3664, 2023 WL 5029899 (N.D. Cal. Aug. 7, 2023)). In *Brown*, the court recognized that "the standing analysis is contextual," and the context of that case was materially different. There, the court denied a motion for summary judgment for lack of standing where plaintiffs had evidence that "Google store[d] users' regular and private browsing data in the same logs; it use[d] those mixed logs to send users personalized ads; and, even if the individual data points gathered are anonymous by themselves, when aggregated, Google can use them to uniquely identify a user with a high probability of success." *Id.* at *6. The court found that was "enough" to "confer standing given the sensitivity" of the private browsing activity at issue, which the court noted could include searching for "health conditions without being stigmatized," "ways to exit a relationship without notifying [an] abuser]," and "date same-sex partners without being outed." *Id.* at *6 n.9. There are no similar allegations in this case.

One final matter on standing. Ms. Cook has not asked for leave to amend (either in her briefing or at oral argument), she did not submit a proposed second amended complaint, and she did not try to explain how another pleading might help her plead standing (indeed, she has taken a position that no amendment is necessary because the kind of information at issue is irrelevant). Her failure in this regard weighs against giving her another chance at supplementing her allegations. *E.g.*,

Davis v. Holder, 994 F. Supp. 2d 719, 727 (W.D. Pa. 2014) (Gibson, J.) (dismissing with prejudice where "Davis has not filed a proposed amendment with the Court nor has he explained how he would amend Count Three of the complaint to allege state action"); *Adelman v. Jacobs*, No. 18-607, 2019 WL 1651612, at *6 (W.D. Pa. Apr. 17, 2019) (Fischer, J.) ("Plaintiffs already filed an amended pleading in this matter and have not affirmatively sought leave to file a second amended complaint nor supplied this Court with a proposed pleading such that leave to amend may be denied on these grounds as well." (citations omitted)). The Court therefore finds that amendment would be inequitable and futile and will grant GameStop's motion to dismiss with prejudice. *See Lightoller*, 2023 WL 3963823, at *5.[4]

II. Ms. Cook has not stated a claim for a violation of the Wiretap Act.

Even if Ms. Cook had standing, she hasn't adequately stated a claim under Pennsylvania's Wiretap Act.[5]

The Wiretap Act, which is patterned after its federal counterpart, the Electronic Communications Privacy Act, 18 U.S.C. § 2510, *et seq.*, prohibits the interception of an electronic communication without prior consent. 18 Pa.C.S. §

[4] Indeed, if Ms. Cook could have amended to plead an injury in fact, she would have. She already amended once. Then, before GameStop filed its second motion to dismiss, she had the chance to amend again, as the Court's procedures require the parties to meet and confer before a motion to dismiss is filed. JUDGE RANJAN'S PRACTICES & PROCEDURES, § II(d). After the motion was filed, she could have amended in response to the motion under Rule 15(a), too. Granting leave to amend at this point would be inequitable.

[5] To survive a motion to dismiss for failure to state a claim, "a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (cleaned up). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* Any reasonable inferences should be considered in the light most favorable to the plaintiff. *See Lula v. Network Appliance*, 255 F. App'x 610, 611 (3d Cir. 2007) (citing *Rocks v. City of Phila.*, 868 F.2d 644, 645 (3d Cir. 1989)).

5725(a).[6] The statute defines "intercept" as the "[a]ural or other acquisition of the ***contents of any*** wire, electronic or oral ***communication*** through the use of any electronic, mechanical or other device." 18 Pa.C.S. § 5702 (emphasis added). "Contents" is defined as "any information concerning the substance, purport, or meaning of that communication." *Id.* So, "contents," in this context, "refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication." *In re Zynga Priv. Litig.*, 750 F.3d 1098, 1106 (9th Cir. 2014) (interpreting Federal Wiretap Act). Thus, determining whether a plaintiff has adequately pled a violation of the statute often comes down to deciding whether the acquired information can best be characterized as either "record information" or "the message conveyed by the communication." *See Goldstein v Costco Wholesale Corp.*, 559 F. Supp. 3d 1318, 1321 (S.D. Fla. 2021) ("The touchtone in many cases arising under [Florida's wiretap statute] and similar statutes is the definition of contents. Courts interpreting contents under the [federal wiretap statute] distinguish between a record or other information pertaining to a customer (known as 'record information') and the contents—*i.e.*, 'substance, purport, or meaning'—of the communication itself." (cleaned up)).

Ms. Cook argues that she "sufficiently alleged the interception of the 'contents' of her Website Communications with GameStop's website" by pointing to six paragraphs in her amended complaint. ECF 31, pp. 15-16 (citing ECF 22, ¶¶ 1, 25,

[6] The Supreme Court has recognized that the Wiretap Act is the "Pennsylvania analog" of the ECPA. *Bartnicki v. Vopper*, 532 U.S. 514, 526 (2001). Because the relevant provisions and statutory definitions (*e.g.*, "intercept" and "contents") from the Wiretap Act are identical to those in the ECPA, the Court can look to decisions applying those provisions and definitions for guidance. *See Com. v. Proetto*, 771 A.2d 823, 829 (Pa. Super. Ct. 2001) *aff'd*, 837 A.2d 1163 (Pa. 2003); *Popa*, 426 F. Supp. 3d at 120-21.

46, 51, 60, 61). Upon close inspection, the Court concludes that there are at least two serious problems with Ms. Cook's core allegations (as she has identified) in this case.

First, Ms. Cook's allegations lack sufficient detail to support a claim. Paragraph 1 comes the closest to giving the Court a starting point for determining whether Ms. Cook has pled the elements of her wiretap claim, but even the allegations in that paragraph come up short. In paragraph 1, Ms. Cook alleges that the code captured her "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[.]" ECF 22, ¶ 1. This allegation, though, lacks critical necessary details for the Court's analysis of the type of information allegedly captured by GameStop's Session Replay Code. What mouse movements? What did she hover over? What did she click? Which keystrokes did she enter? What kind of webpages did she visit? All this information should be available to Ms. Cook; after all, she is the one who allegedly browsed GameStop's website. But it is absent from the amended complaint.

The allegations in several of the other paragraphs cited by Ms. Cook are problematic because they aren't specific to GameStop. For example, the allegations in paragraph 25 set forth claims about how Session Replay Code works "in general"—notably absent are any specific allegations about whether ***GameStop's*** code operated in the manner described. ECF 22, ¶ 25 (conceding that the "types of events captured by Session Replay Code vary by specific product and configuration, but in general are wide-ranging and can encompass virtually every user action[.]"). The same is true for Paragraphs 46 and 51, which merely describe the capabilities of Clarity. *Id.* ¶¶ 46, 51. Missing are allegations about how ***GameStop*** implemented Clarity.

It's not enough for Ms. Cook to allege the potential capabilities of the Session Replay Code. Rather, she needed to allege that GameStop, in fact, harnessed the capabilities she describes, and it had the result of capturing the contents of specific

communications. But she did not do that. *E.g.*, *id.* ¶¶ 25 ("The Types of events captured by Session Replay Code ***vary by specific product and configuration***" (emphasis added)), 28 (regarding Session Replay Code, "researchers have found that a variety of highly sensitive information ***can be*** captured in event responses from website visitors" (emphasis added)), 29 ("Session Replay Code ***may*** capture data that the user did not even intentionally transmit to a website during a visit" (emphasis added)), 30 ("Session Replay Code ***does not necessarily anonymize user sessions***" (emphasis added)), 49 ("***Clarity offers three standard approaches*** when it comes to masking sensitive information collected from a user's interaction with a website" (emphasis added)).

The allegations in the remaining paragraphs aren't connected to Ms. Cook. Paragraph 61 describes information captured by Clarity from an unidentified visitor to GameStop's website, but Ms. Cook does not plead facts that would allow the Court to conclude that she engaged in similar activity on GameStop's website. *Id.* ¶ 61.

The result of these pleading deficiencies is that the Court is forced to speculate about how GameStop's Session Replay Code was configured and operated and how Ms. Cook's visits to GameStop's website unfolded, which it cannot do.

Second, even giving the most liberal construction to Ms. Cook's allegations and construing all inferences in her favor, the allegations are not enough to state a wiretap claim. Recall, Ms. Cook claims that she "communicated with GameStop's website by using her mouse to hover and click on certain products and typing search words into the search bar." *Id.* ¶ 58. She also allegedly "selected a product to add to her shopping cart," but did not complete the purchase. *Id.* Broken down into three categories, then, Ms. Cook alleges GameStop "intercepted" her mouse movements and clicks, keystrokes, and URLs of web pages visited. *Id.* ¶ 1. None of this information constitutes the "content" of "communications."

Mouse movements and clicks. When a website user moves the cursor or clicks the mouse, it does not plausibly reveal the substance of any communication. It could be construed, at most, in two ways. First, as the kind of "routing information" that has historically not been recognized as content. When a user moves his or her mouse and clicks on a link, that click is a request for the computer to take the user to a specific location within the webpage's architecture. Navigating through a website's multiple pages is not the substance of a communication; it's an action taken to go to a digital location.

Alternatively, these mouse movements and clicks could be considered "the cyber analog to record information [GameStop] could have obtained through a security camera at a brick-and-mortar store." *Goldstein*, 559 F. Supp. 3d at 1321. That is, these movements and clicks literally constitute a record of her movements within a digital space. Any "substance" that can flow from these movements must be inferred from the observer, and are therefore not communicative.

Consider a customer at one of GameStop's brick-and-mortar stores. If a customer walked over to a section of the store devoted to sports video games, that could mean the customer was interested in sports video games, but it could also mean any number of other things. The customer could just be wandering around the store. Or the customer could be admiring the photograph of the cover athlete for the game because that player plays for the customer's favorite team, but the customer has no interest in purchasing or learning more about the game itself. The point is that the customer isn't intending to communicate anything to anyone by walking around the store. He or she is just walking around the store. The observer must guess at what, if anything, those movements mean. The same thing goes for a website visitor's

navigation around a website. That's what differentiates this kind of activity from a substantive communication like a verbal conversation or text message.[7]

URLs. Ms. Cook also alleges that GameStop captured a record of the URLs of web pages she visited while on GameStop's site. ECF 22, ¶ 1. A URL is a Uniform Resource Location, "used to identify the physical location of documents on servers connected to the internet." *In re Nickelodeon Cons. Priv. Litig.*, No. 12-7829, 2014 WL 3012873, at *15 (D.N.J. July 2, 2014) (cleaned up). Location identifiers, like URLs, "have classically been associated with non-content means of establishing communication." *In re Google Inc. Cookie Placement Cons. Priv. Litig.*, 806 F.3d 125, 136 (3d Cir. 2015) (cleaned up). That's because they are usually "addressing information and do not necessarily reveal any more about the underlying contents of communications than do phone numbers." *In re Zynga*, 750 F.3d at 1108 (cleaned up). But that's not to say URL information could never be considered the substance of a communication. "Under some circumstances, a user's request to a search engine for specific information could constitute a communication such that divulging … that search term to a third party could amount to disclosure of the contents of a communication." *Id.* at 1108-09; *see also In re Google*, 806 F.3d at 139 ("[W]e are persuaded that—at a minimum—some queried URLs qualify as content."). So, in the final calculus, "whether a URL involves 'contents'" depends "on how much information would be revealed by disclosure of the URL." *In re Google*, 806 F.3d at 138.

The Court simply has no way of knowing that information based on the amended complaint. Ms. Cook pleads that she typed "search words into the search

[7] Ms. Cook argues that these movements and the rest of her interactions are like her calling the store and asking for information. ECF 43, 24:13-25:14. That analogy falls flat. A phone call is different in that on a phone call, one side of the conversation must speak and communicate substance to the other side or else the conversation will not function.

bar," but doesn't say what those searches were, whether she hit "enter" after typing the searches, and whether that action generated a new URL that could be recorded by the Session Replay Code.[8] At most, then, the Court can only reasonably infer that the URLs corresponded to different physical locations of pages, documents, and files on GameStop's servers, which is the kind of non-content information that is not covered by the Wiretap Act.

Keystrokes. Ms. Cook generically alleges that her "keystrokes" were recorded, but the Court has no idea what those keystrokes could be, other than the search words mentioned above. Because that crucial information is not pled in the amended complaint, the Court cannot find that these "keystrokes" amounted to the content of a communication.

Ms. Cook's rebuttal to the analysis above is to broadly argue "[e]verything about what happens in your interaction with the website is communicative in nature." ECF 43, 59:8-9. In short, it's Ms. Cook's position that "[o]nce you're on the website, you've communicated." *Id.* at 59:11-12. But there's simply no support for this position in the caselaw,[9] and it contradicts the reality of how websites operate.

---

[8] Ms. Cook's screenshot supposedly showing information that Clarity captured from an unidentified www.gamestop.com visitor doesn't change the analysis. ECF 22, ¶ 61. That screenshot is not connected to anything that Ms. Cook did on GameStop's website and it's not even clear what that screenshot represents because Ms. Cook hasn't provided enough context. *Id.*

[9] Ms. Cook's citation to *Oliver v. Noom, Inc.*, No. 2:22-cv-1857 (W.D. Pa.) (Stickman, J.) does not help her cause. ECF 44. The alleged information that was intercepted in that case was wholly different—there, the plaintiff alleged that the defendant "collected personal information she input[ted] as part of Noom's 10-minute online quiz, including her height, weight, gender, age, reason for wanting to lose weight, how active she is, how often she eats, and whether she is at risk for specific health issues." ECF 44-1, p. 14. Those kinds of affirmative survey responses revealing highly personal information did communicate substance to the defendant. That kind of particularized allegation is absent here, though.

And such an expansive interpretation would impermissibly render the distinction between content and non-content in the statute superfluous. *United States v. Cooper*, 396 F.3d 308, 312 (3d Cir. 2005) ("It is a well-known canon of statutory construction that courts should construe statutory language to avoid interpretations that would render any phrase superfluous." (cleaned up)). Thus, Ms. Cook has failed to state a claim under the Wiretap Act.[10]

III. Ms. Cook has not stated a claim for intrusion upon seclusion.

To state a claim for intrusion upon seclusion under Pennsylvania law, a plaintiff must show that a defendant "intentionally intrude[d], physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns," and that "the intrusion would be highly offensive to a reasonable person." *Popa*, 426 F. Supp. 3d at 120 (quoting Restatement (Second) of Torts § 625B). For an invasion to give rise to an actionable claim for intrusion upon seclusion, it must be "of the sort which would cause mental suffering, shame, or humiliation to a person of ordinary sensibilities." *Chicarella v. Passant,* 494 A.2d 1109, 1114 (Pa. Super. Ct. 1985) (cleaned up).

Ms. Cook's claim fails at the outset because, as discussed above, there's no allegation that GameStop intruded upon her "private affairs or concerns." And even

[10] The Court is not granting leave to amend because the principal basis for dismissal is lack of standing, and as noted above, it would be futile and inequitable to allow amendment on that issue. As to the alternative ground for dismissing the Wiretap Act claim, the Court is not convinced that Ms. Cook can or even would want to amend to correct these core deficiencies. In response to GameStop's first motion to dismiss, Ms. Cook amended her allegations. ECF 22. That first motion to dismiss raised identical issues to those addressed by the Court in this Opinion. *See* ECF 15. It's no surprise, then, that the nature of Ms. Cook's interactions with the website, as pled by her, would be critical to the Court's analysis of this motion. Yet she failed to come back with the kind of detail on specific communications that might state a plausible claim. That was clearly a tactical decision. Allowing Ms. Cook to alter her tactics by amending the complaint and forcing GameStop to respond to further amendment would be inequitable.

if the information could fit into the category of private information, the collection and disclosure of a website visitor's activity does not constitute the highly objectionable conduct needed to state a claim. *See, e.g.*, *In re Nickelodeon*, 827 F.3d at 294-95 (use of third-party tracking cookies on a website geared towards children not offensive enough to withstand a motion to dismiss); *In re Google, Inc. Priv. Pol'y Litig.*, 58 F. Supp. 3d 968, 988 (N.D. Cal. 2014) (no intrusion upon seclusion claim where Google collected and disclosed users' data, including their browsing histories). Nor has Ms. Cook alleged how GameStop's use of Session Replay Code caused her "mental suffering, shame, or humiliation." The allegations in the amended complaint simply do not pass muster as to this claim.

CONCLUSION

For these reasons, it is hereby **ORDERED** that GameStop's motion to dismiss (ECF 25) will be **GRANTED**, and the amended complaint will be dismissed with prejudice. An appropriate order follows.

Date: August 28, 2023

BY THE COURT:

/s/ J. Nicholas Ranjan
United States District Judge