UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

----------X

BRIAN MOUNT and THOMAS NAIMAN, individually and on behalf of other similarly situated persons,

Plaintiffs,

- against -

PULSEPOINT, INC.,

Defendant.

----------X

MEMORANDUM AND ORDER

13 Civ. 6592 (NRB)

NAOMI REICE BUCHWALD
UNITED STATES DISTRICT JUDGE

Plaintiffs Brian Mount and Thomas Naiman (collectively, "plaintiffs") contend that defendant PulsePoint, Inc. ("PulsePoint") circumvented their default browser settings in order to set tracking cookies on their devices. They have initiated this putative class action bringing claims under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030, New York General Business Law § 349 ("GBL § 349"), and New York common law on behalf of Safari users in the United States between June 1, 2009, and February 29, 2012 (the "Class Period"), whose privacy controls were set to block third-party advertiser cookies and who visited a website that placed a PulsePoint cookie on their device. PulsePoint has moved to dismiss plaintiffs' amended complaint pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). For the following reasons, we deny the Rule 12(b)(1) motion and grant the Rule 12(b)(6) motion.

BACKGROUND

The following facts, which we assume to be true for purposes of this motion, are drawn from plaintiffs' amended complaint (or "FAC") and the July 23, 2013 consent order entered into by PulsePoint and the Attorney General of New Jersey attached thereto.

I. Cookies and Targeted Advertising

Many courts, including this one, have previously written on internet cookie technology and the role of third-party cookies in targeted advertising, see, e.g., In re: Nickelodeon Consumer Privacy Litig., --- F.3d ---, No. 15-1441, 2016 WL 3513782, at *2 (3d Cir. June 27, 2016) ("Nickelodeon"); In re Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125, 130-31 (3d Cir. 2015) ("Google"); In re DoubleClick Inc. Privacy Litig., 154 F. Supp. 2d 497, 503-05 (S.D.N.Y. 2001) ("DoubleClick"), and we provide here only an abbreviated summary, adopted from the amended complaint, for context. Typically, many of the ads visible on a particular webpage are not selected and delivered by the website visited by the user itself. Instead, a webpage may have one or more inline frames, referred to as "iframes," and a website with extensive advertising will often contract with third-party digital advertising companies such as PulsePoint to serve ads in these iframes directly from the third party's server. FAC ¶¶ 17, 19.

Not surprisingly, advertisers are willing to pay more to fill an iframe with a targeted ad to a "known" internet user visiting

a webpage than they are willing to pay to deliver an ad to an unknown user. Id. ¶ 17. Online advertising companies are thus strongly incentivized to gather information on internet users; much of this is accomplished by use of "cookies." Id. ¶ 18.

Cookies are small text files that a web server places on a user's computing device. Among other uses, they permit a website to "remember" information about a user, such as the items in a virtual shopping cart. Id. ¶ 15. Cookies are generally classified as either session cookies or persistent cookies. Id. ¶ 18. Session cookies are transitory and are used only to help navigate the website currently being visited. A session cookie is normally erased when the browser is closed. Id. Persistent cookies, commonly called "tracking cookies," are designed to remain after the user moves on to a different website or even after the browser is closed. Id. These cookies can stay on a device for months or years, and may be used to help a website identify a unique browser returning to the site. Id.

The parties also distinguish between first-party and third-party cookies. While the former are set on a user's device directly by the website the user visited, the latter are set by third parties, including advertising companies that have placed ads on the first-party website. Id. ¶¶ 25-28. By reading and matching tracking cookies they have placed on a user's device, third-party advertising companies can create digital profiles of

internet users based on their browsing activities. Id. ¶¶ 18-20.

II. Safari's Default Settings

Apple launched its Safari browser in 2003. FAC ¶ 23. Sensing the public's growing awareness of web tracking and desire for increased privacy protection, Apple decided to offer to block cookies from third parties as a default setting. Id. ¶ 24. This feature is still advertised by Apple: its website for Safari notes that third-party cookies "can be used to track where you go on the web, target you with ads, or create a profile of your online activities," and touts the fact that "Safari was the first browser to block these cookies by default." Id. During the Class Period, the default setting for Safari on computers, iPhones, and iPads was to block third-party cookies while accepting cookies from sites visited. Id. ¶¶ 24-29.

III. PulsePoint Places Third-Party Cookies on Safari Browsers

PulsePoint, headquartered in New York and incorporated in Delaware, is a digital media company engaging in consumer analytics and ad-serving across various platforms. FAC ¶ 14. The company was formed in 2011 through a merger of ContextWeb, Inc. ("ContextWeb"), and Datran Media Corp. Id. During the Class Period, ContextWeb, and subsequently PulsePoint, operated an ad exchange which served as an intermediary between website publishers selling ad space and advertisers seeking to advertise on the publishers' websites. Id.

At some point, ContextWeb developed a workaround of Safari's default cookie-blocking setting. Plaintiffs contend that through this workaround, ContextWeb, and later PulsePoint, were able to effectively track and monitor the prospective class members' web surfing in real time and intercept "Personally Identifiable Information," which they sold to advertisers who could better target ads to class members based on their browsing habits. Id. ¶ 4.

Plaintiffs largely rely on the July 2013 consent order entered into by PulsePoint and the New Jersey Attorney General resolving, without formal charges, an investigation by the New Jersey Division of Consumer Affairs into PulsePoint's alleged violations of the New Jersey Consumer Fraud Act. Id. ¶ 35. In the consent order, PulsePoint admits that between June 2009 and February 2012, PulsePoint and its predecessor ContextWeb employed a JavaScript code in the ads they placed on websites to set cookies on Safari browsers whose privacy settings were arranged to block third-party cookies. Id. ¶ 37. The code included a mechanism replicating a submission of a particular "form" that made Safari act as if the user had clicked on the ad on a webpage, when in fact the user had not. Id. As a result, Safari would permit PulsePoint to place cookies on the user's device. Id.

However, besides its conclusory reference to users' "Personally Identifiable Information," id. ¶ 4, the amended

complaint does not specify what information other than web browsing history PulsePoint was able to acquire or how PulsePoint was able to acquire it. The consent order explains that PulsePoint's cookies could be used to "uniquely identify[] a user's browser or computer," FAC, Ex. A ¶ 4, but there are no factual admissions in the consent order suggesting that PulsePoint was attempting to link browsing information to the specific individual(s) using the browser. At oral argument, plaintiffs confirmed that they do not allege that PulsePoint was able to associate any information it collected or maintained on Safari users with their actual identities. See Transcript of June 16, 2016 Oral Argument ("Oral Arg. Tr.") at 8-9 (stating that algorithms can theoretically discern the actual identity of a browser user based on aggregating sufficient browsing information but conceding no such allegations made in this case).

Instead, plaintiffs focus on PulsePoint's alleged ability to aggregate sites visited by a particular browser or device. One cookie ContextWeb and PulsePoint placed on class members' devices was a "*pb_rtb_ev*" network synchronization cookie, which was used to allow third-party ad buyers to identify their cookies on PulsePoint's network. FAC ¶ 37. If the third-party ad buyer had also set its own cookie on the class member's device, the buyer was able to synchronize that user's cookies. Id. Plaintiffs believe this cookie, found on over 1,000 websites during the Class

Period, allowed PulsePoint and/or third-party ad buyers to associate the web browsing of a single browser and/or device over multiple websites. Id. ¶¶ 37, 42; Oral Arg. Tr. at 5-7.

Also a subject of the consent order is the privacy policy PulsePoint's predecessor ContextWeb had in effect prior to August 2011, which stated:

> You can generally configure your browser to accept all cookies, reject all cookies, or notify you when a cookie is set. (Each browser is different, so check the 'Help' menu of your browser to learn how to change your cookie preferences).

FAC ¶ 37. Plaintiffs accuse ContextWeb of inaccurately describing Safari's functionality, as ContextWeb (and later PulsePoint) placed cookies on devices of Safari users whose settings had been set to block cookies from third-parties. Id.[1]

The consent order required PulsePoint to agree to a $1 million settlement payment. Id. ¶ 39. The company also agreed to certain other conditions, including maintaining systems for two years configured to instruct Safari browsers to expire any offending cookies, updating its website to better describe its privacy policies, and implementing a five-year program featuring privacy controls and procedures. Id. ¶¶ 38-39; FAC Ex. A ¶¶ 22-31.

[1] According to the consent order, PulsePoint continued this practice until February 2012, when independent researchers published an online report revealing that other companies were exploiting the same feature of Safari. FAC, Ex. A ¶ 10; see Jonathan Mayer, Safari Trackers, WEB POLICY (Feb. 17, 2012), http://webpolicy.org/2012/02/17/safari-trackers/. PulsePoint represented to the New Jersey Attorney General that its directors and officers were unaware of the conduct in question until February 2012. FAC, Ex. A ¶ 11.

IV. Procedural History

Plaintiffs Mount and Naiman each used Safari with its default settings and visited websites with PulsePoint-placed third-party ads during the Class Period. FAC ¶¶ 12-13. Mount, who is domiciled in New Jersey, used Safari on his mobile device, whereas Naiman, who is domiciled in New York, used it on his computer. Id. ¶¶ 12-13, 52.

In 2013, they commenced this putative class action, bringing a number of federal and state law claims against PulsePoint. We stayed the proceedings pending a ruling by the Third Circuit in Google, 806 F.3d 125, which involved very similar allegations and claims brought under the same federal statutes. In November 2015, the Third Circuit affirmed the dismissal of the federal claims and certain claims brought under California law in that action. Google, 806 F.3d at 135-49, 152-53. However, it also vacated the dismissal of privacy claims brought under the California Constitution and California tort law. Id. at 149-52. Following Google, we lifted the stay and granted plaintiffs leave to amend. The amended complaint dropped claims brought under the Wiretap Act and Stored Communications Act, but retained all other claims.

DISCUSSION

PulsePoint now moves to dismiss the amended complaint pursuant to Rule 12(b)(1) on the ground that it fails to plead the

injury in fact required for Article III standing, and pursuant to Rule 12(b)(6) on the ground that it fails to state any claim upon which relief may be granted.

I. Rule 12(b)(1) Motion to Dismiss

When, as here, a defendant has brought a facial Rule 12(b)(1) motion, meaning a motion "based solely on the allegations of the complaint or the complaint and exhibits attached to it," we accept as true all the material factual allegations of the complaint and draw all reasonable inferences in favor of the plaintiffs. Carter v. HealthPort Techs., LLC, 822 F.3d 47, 56-57 (2d Cir. 2016). The burden is on the plaintiffs to allege facts that "affirmatively and plausibly suggest" that they have standing to sue, Amidax Trading Grp. v. S.W.I.F.T. SCRL, 671 F.3d 140, 145 (2d Cir. 2011), and to "demonstrate standing for each claim and form of relief sought," Carver v. City of New York, 621 F.3d 221, 225 (2d Cir. 2010) (internal quotation marks omitted). Furthermore, the named plaintiffs "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 and which they purport to represent." Simon v. Eastern Ky. Welfare Rights Org., 426 U.S. 26, 40 n.20 (1976) (internal quotation marks omitted).

The three elements of constitutional standing are (1) "an injury in fact," which is "an invasion of a legally protected interest which is (a) concrete and particularized and (b) actual

or imminent, not conjectural or hypothetical"; (2) "a causal connection between the injury and the conduct complained of"; and (3) a likelihood, as opposed to mere speculation, "that the injury will be redressed by a favorable decision." Lujan v. Defenders of Wildlife, 504 U.S. 555, 560–61 (1992) (internal quotation marks and citations omitted). While we must assure ourselves that each of these elements is met, PulsePoint's motion focuses only on the first.

Recently, in Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1548 (2016), the Supreme Court underscored the necessity of satisfying each independent requirement of Article III injury in fact. Thus, in addition to being actual or imminent, an alleged injury must be both "particularized," i.e., "affect the plaintiff in a personal and individual way," Lujan, 504 U.S. at 598 n.1, and "concrete," i.e., "real, and not abstract," Spokeo, 136 S. Ct. at 1548 (internal quotation marks omitted). However, "real" does not necessarily mean "tangible," and intangible injuries, while perhaps more difficult to recognize, can also be concrete. Id. at 1549. In considering whether an alleged intangible harm is concrete, the Spokeo Court emphasized the importance of looking to whether it "has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts," and to whether Congress has identified it as a harm meeting the minimum Article III requirements. Id.

A. Actionable Theories of Injury

We believe the Article III requirements are met with respect to two of the harms claimed by plaintiffs. To begin, plaintiffs' asserted loss of privacy is particularized: they allege that PulsePoint deployed code in ads that caused the Safari browsers on their devices to "drop[] the default protection and accept[] tracking cookies," FAC ¶ 3, and that PulsePoint was able to sell information collected through use of these cookies to advertisers, see id. ¶¶ 1, 4, 37. This alleged harm is also sufficiently concrete. Recognizing the linkage of "concrete" "intangible" injuries to those traditionally regarded as "providing a basis for a lawsuit," Spokeo, 136 S. Ct. at 1549, we believe plaintiffs' allegations are sufficiently grounded in the harm protected against by the common law tort of intrusion upon seclusion so as to constitute legally cognizable injury, see Nickelodeon, 2016 WL 3513782, at *23-25 (allegations that defendant collected information through use of cookies despite promising that it did not collect personal information sufficient to state privacy claim under New Jersey law); Google, 806 F.3d at 149-52 (allegations that defendant circumvented cookie blocker despite announcing that internet users could reset browsers to refuse all cookies sufficient to state privacy claim under California law); see also Mey v. Got Warranty, Inc., --- F. Supp. 3d ---, No. 5:15-CV-101, 2016 WL 3645195, at *3 (N.D. W. Va. June 30, 2016) ("Invasion of

privacy is . . . an intangible harm recognized by the common law."); Leung v. XPO Logistics, Inc., No. 15 C 03877, 2015 WL 10433667, at *5 (N.D. Ill. Dec. 9, 2015) (alleged aggravation and invasion of privacy resulting from unwanted phone call enough to confer standing even though injuries did not necessarily give rise to a cause of action).

In addition, plaintiffs' allegations give rise to another particularized and concrete harm. While we conclude below that plaintiffs have failed to allege any significant level of consumption of device capacity or any discernible interference with device performance, we believe that PulsePoint's alleged unauthorized setting of cookies on plaintiffs' devices is itself injury in fact. We may reasonably infer from the amended complaint that any set cookies had a marginal, even if *de minimis* and imperceptible, effect on the operation of those devices. FAC ¶ 34. Proffered as the basis for, inter alia, plaintiffs' common law trespass to chattels claim, these allegations support standing, even if they do not ultimately plausibly establish the level of interference with the "intended functioning" of the devices "necessary to establish a cause of action for trespass," In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1069 (N.D. Cal. 2012). See also In re Methyl Tertiary Butyl Ether ("MTBE") Products Liab. Litig., 725 F.3d 65, 105 (2d Cir. 2013) (distinguishing between "threshold question" of constitutional

standing and injury actionable under New York tort law (internal quotation marks omitted)).

These two injuries are fairly traceable to PulsePoint's conduct and would likely be redressed by a favorable ruling from this Court, and accordingly, PulsePoint's motion to dismiss pursuant to Rule 12(b)(1) is denied.

B. Non-Actionable Theories of Injury

Because plaintiffs' inability to plead particularized and concrete injury based on their remaining theories of harm support our ultimate dismissal of their claims on the merits, we address these other theories first.

First, plaintiffs contend that they were injured because tracking cookies burden computers' limited memory and storage capacity and consume a substantial portion of browsers' efforts when loading websites. Specifically, they allege that "web tracking imposes substantial costs on internet users by clogging the users' Devices with hundreds of unwanted cookies, which in turn trigger a cascade of unwanted communications between the Device and various online companies." FAC ¶ 34 (emphases added). Incorporated into the amended complaint is a graphic from a cookie-blocking software company stating that 26.3% of a browser's effort when loading a website is consumed by responding to requests for personal information triggered by tracking cookies. Id. This level of unwanted communication significantly slows down browser

performance and increases CPU usage. Id.

Even if the above plausibly suggests some unspecified effect from any marginal increase in cookies on plaintiffs' devices as a result of PulsePoint's Safari workaround, the generalized recital of the "substantial costs" of tracking cookies experienced by "users" does not suggest named plaintiffs suffered these costs. Assuming Naiman's and Mount's Safari browsers accepted PulsePoint cookies, the amended complaint is devoid of any additional facts indicating that either individual personally had "hundreds of unwanted cookies" placed on his device by PulsePoint such that a "cascade of unwanted communications" was triggered. Indeed, although the amended complaint alleges that Naiman and Mount visited websites with third-party ads placed by PulsePoint, it provides no indication as to how frequently those websites were visited or how many ads on those websites were served by PulsePoint. More importantly, it is nowhere alleged that either Naiman or Mount suffered slower browser performance or increased CPU usage. Indeed, at oral argument, plaintiffs' counsel confirmed that they had never asked their clients if they experienced such problems during the Class Period.[2] Accordingly, we cannot infer

[2] See Oral Arg. Tr. at 10-11 ("THE COURT: They have never articulated [a] contemporaneous reaction that their computer or iPhone was not behaving as well as it should up to its technological capacity? MR. STRAITE: That's correct in this complaint, your Honor. . . . THE COURT: The bottom line is your clients never said to you, I just didn't feel that my computer or my iPhone was working as fast as it should be or mysteriously I ran out of capacity or something like that? MR. STRAITE: We never inquired into that, right, your Honor."). Plaintiffs' counsel noted that there was no record of PulsePoint's offending

that named plaintiffs experienced any appreciable burden on device capacity or interference with normal device functioning.

Second, plaintiffs argue that they were injured by the misappropriation of the value of their browsing histories. They allege that "personal information has real monetary value to the user" and "online advertisers" alike. FAC ¶¶ 31-32. Noting that individuals can receive cash for having their web browsing monitored through programs offered by Google and Microsoft, plaintiffs contend that PulsePoint's harvesting of browsing information without compensation represents "real out-of-pocket loss." Id. ¶ 32.

While we recognize that browsing information may possess value in the abstract, absent allegations suggesting that plaintiffs' ability to monetize their browsing information was diminished, this alleged harm remains too conjectural. The Third Circuit in Google persuasively rejected similar allegations in analyzing whether the plaintiffs had pled statutory "loss" under the CFAA:

> The complaint plausibly alleges a market for internet history information such as that compiled by the defendants. Further, the defendants' alleged practices make sense only if that information, tracked and associated, had value. However, when it comes to showing "loss," the plaintiffs' argument lacks traction. They allege no facts suggesting

cookies on any devices because PulsePoint agreed to expire them as a condition of the consent order with the New Jersey Attorney General. See id. However, whether or not counsel could determine if PulsePoint's cookies actually appeared on Naiman's or Mount's device, they were still free to ask them if they had experienced any diminished performance during the Class Period.

> that they ever participated or intended to participate in the market they identify, or that the defendants prevented them from capturing the full value of their internet usage information for themselves. For example, they do not allege that they sought to monetize information about their internet usage, nor that they ever stored their information with a future sale in mind. Moreover, the plaintiffs do not allege that they incurred costs, lost opportunities to sell, or lost the value of their data as a result of their data having been collected by others.

806 F.3d at 149.

The amended complaint suffers from the same deficiencies. For instance, while plaintiffs reference programs compensating individuals in exchange for monitoring their web browsing, they do not allege that they are unable to participate in or would receive less compensation from such programs as a result of PulsePoint's conduct. From the limited allegations put forward on this subject, the Court cannot reasonably infer either conclusion.

Plaintiffs respond that they do not need to plead that their ability to monetize their data was diminished, as it is enough to allege that the data was misappropriated. For this proposition, they rely on inapposite cases involving misappropriation of confidential business information. Thus, the Seventh Circuit in FMC Corp. v. Boesky found that the plaintiff corporation had suffered a cognizable injury to its "property right" in keeping confidential and making exclusive use of information concerning its business plans when the information was exploited by others for insider trading purposes. 852 F.2d 981, 990-91 (7th Cir.

1988); see United States v. O'Hagan, 521 U.S. 642, 654 (1997) ("A company's confidential information qualifies as property to which the company has a right of exclusive use . . . ."). To emphasize why the violation of this right constituted injury, the Seventh Circuit directly linked the secrecy of the information to its commercial value, explaining that its misappropriation "destroyed whatever value it had in FMC's hands." FMC Corp., 852 F.2d at 991 & n.21. Similarly, in I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc., this Court held that a plaintiff adequately pled CFAA damages based on allegations that the defendant accessed certain data intended to be available only to the plaintiff's customers and copied the data for a competing service. 307 F. Supp. 2d 521, 523, 525 (S.D.N.Y. 2004).

These cases bear no relation to the allegations here. Naiman and Mount do not assert a property right in the exclusive use of their browsing information. Furthermore, in the above cases, exclusive use of the information was critical to its commercial value to the plaintiff businesses, and unauthorized disclosure to others risked harming the plaintiffs' ability to capitalize on that value. As discussed already, Naiman and Mount fail to explain how PulsePoint's collection of their historical browsing information would have a similar effect.[3]

[3] Plaintiffs also rely on In re Anthem, Inc. Data Breach Litig., --- F. Supp. 3d ---, No. 15-MD-02617-LHK, 2016 WL 589760 (N.D. Cal. Feb. 14, 2016) ("Anthem"), which held that loss in the value of certain personal information

II. 12(b)(6) Motion to Dismiss

In ruling on a Rule 12(b)(6) motion, we again accept as true all factual allegations in the complaint and draw all reasonable inferences in the plaintiffs' favor. Harris v. Mills, 572 F.3d 66, 71 (2d Cir. 2009). We are "constrained, however, to ascertain that the 'complaint contain sufficient factual matter, accepted as true, to state a claim to relief that is plausible on its face.'" DiFolco v. MSNBC Cable L.L.C., 622 F.3d 104, 111 (2d Cir. 2010) (quoting Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009)). A claim is facially plausible "when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Iqbal, 556 U.S. at 678.

after a data breach affecting a health benefits and insurance company constituted actual harm for purposes of pleading a GBL § 349 claim. However, the Anthem Court's reasoning focused on the increased risk of misuse of the data, which encompassed information such as Social Security and health care ID numbers. 2016 WL 589760, at *2, *25-27; see id. at *26 (emphasizing allegations that cyberattackers had extracted and misused information, including by filing a false tax return); see also In re Anthem, Inc. Data Breach Litig., No. 15-MD-02617-LHK, 2016 WL 3029783, at *15 (N.D. Cal. May 27, 2016) ("Anthem II"). The imminent threat following a data breach of misuse of personal data, which misuse may include fraudulent charges and identity theft, is a theory of injury distinct from plaintiffs' theory of owed compensation for browsing information. Although Anthem II held that pleading the existence of an "economic market" for plaintiffs' hacked personal information was sufficient to constitute actual harm, id., we find that holding unpersuasive to the extent it is disassociated from the particular risks related to data breaches. See Khan v. Children's Nat'l Health Sys., --- F. Supp. 3d ---, No. TDC-15-2125, 2016 WL 2946165, at *4-6 (D. Md. May 19, 2016) (in data breach case, considering alleged harms from increased risk of identity theft and diminished value of personally identifiable information separately; latter theory of harm failed to support injury in fact where plaintiff did not explain how hackers' possession of her information diminished its value and did not claim she would ever sell her information).

A. The CFAA Claim

According to plaintiffs, PulsePoint violated the CFAA in three ways: by "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] . . . information from any protected computer," by "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer," and by "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss," 18 U.S.C. § 1030(a)(2)(C), (a)(5)(A), (a)(5)(C). While "primarily a criminal statute designed to combat hacking," WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 201 (4th Cir. 2012), the CFAA also permits a private party "who suffers damage or loss by reason of a violation of [the statute]" to bring a civil action "to obtain compensatory damages and injunctive relief or other equitable relief," 18 U.S.C. § 1030(g).

A person who suffers "damage or loss" may bring a civil action for a CFAA violation "only if the conduct involves 1 of the factors set forth in" § 1030(c)(4)(A)(i)(I)-(V). Id. § 1030(g). The sole factor implicated here is factor (I): "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value." In their briefing, Naiman and Mount argue only that they suffered "damage," defined under the CFAA as "any impairment to

the integrity or availability of data, a program, a system, or information," id. § 1030(e)(8). They contend that PulsePoint caused such "damage" by burdening their devices' resources, disabling their browsers' cookie blockers, and misappropriating their personal data.

However, the relevant "conduct" factor requires plaintiffs to allege "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value," id. § 1030(c)(4)(A)(i)(I) (emphasis added). Under the CFAA, "'loss' means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service." Id. § 1030(e)(11). Accordingly, even if plaintiffs successfully allege "damage," they must allege that they suffered at least $5,000 in "loss" as well. See Czech v. Wall St. on Demand, Inc., 674 F. Supp. 2d 1102, 1110, 1121 (D. Minn. 2009) (required element for plaintiffs suing for conduct involving factor (I) to plead "loss" of $5,000 or more).

PulsePoint contends that plaintiffs have not pled CFAA "damage" or "loss," and have not pled "loss" over $5,000. We have already rejected the argument that the alleged misappropriation of data caused plaintiffs economic harm. Further, we have found that any allegations of discernible adverse effects on device

performance were too generalized to constitute injury to named plaintiffs. Even assuming some additional "burden" on processing power or browser speed resulting from any PulsePoint cookies we may infer were placed on plaintiffs' devices, courts have regularly rejected similar attempts to plead CFAA damages based on such bare allegations of consumption of limited resources. See, e.g., iPhone Application Litig., 844 F. Supp. 2d at 1066-67 (rejecting argument that CFAA damages requirement met by allegations of consumption of memory space); Del Vecchio v. Amazon.com, Inc., No. C11–366-RSL, 2011 WL 6325910, at *4 (W.D. Wash. Dec. 1, 2011) (finding plaintiffs failed to meet loss threshold where they had not alleged any discernible difference in computer performance while visiting defendant's site).

Plaintiffs' last theory of "damage" is that the Safari browser itself was impaired when their default privacy settings were circumvented by PulsePoint's cookies. However, plaintiffs do not allege that they incurred any "loss" contemplated by the statutory definition, such as repair or restoration costs, as a result of that impairment. See Nexans Wires S.A. v. Sark-USA, Inc., 319 F. Supp. 2d 468, 475 (S.D.N.Y. 2004) (loss within meaning of § 1030(e)(11) "means any remedial costs of investigating the computer for damage, remedying the damage and any costs incurred because the computer cannot function while or until repairs are made"), aff'd, 166 F. App'x 559 (2d Cir. 2006). Accordingly,

plaintiffs fail to plead the requisite $5,000 "loss."

Even if the monetary threshold could be satisfied by alleging "damage" alone, plaintiffs have not done so here. The amended complaint does not attempt to ascribe any value to Safari's default cookie-blocking settings. Nor does it allege that Naiman or Mount paid for Safari. Plaintiffs have not pled any facts from which we could infer that the alleged "impairment" to their browsers caused quantifiable damages of $5,000 over a one-year period.

They fare no better even if, as they contend, we may aggregate alleged damages across prospective class members. This Court has previously held that for purposes of the $5,000 threshold, damages "may only be aggregated across victims and over time for a single act." DoubleClick, 154 F. Supp. 2d at 523. In the same decision, we held that, because the relevant CFAA subsection makes it a violation to "intentionally access[] a computer without authorization . . . and thereby obtain[] . . . information," the prohibited act turns on the "the perpetrator's access to a particular computer," and thus the plaintiffs in that action could not aggregate damages resulting from the defendant's "accessing of cookies" on millions of computers. DoubleClick, 154 F. Supp. 2d at 524 (emphases in original) (quoting 18 U.S.C. § 1030(a)(2)(C)). Since then, the CFAA has been amended four times. However, we need not determine whether to revisit those portions of DoubleClick here: the lack of any pled economic harm resulting from the

"impairment" to Safari precludes us from aggregating that harm across any putative class, see Yunker v. Pandora Media, Inc., No. 11-CV-03113 JSW, 2013 WL 1282980, at *10 (N.D. Cal. Mar. 26, 2013); LaCourt v. Specific Media, Inc., No. SACV 10-1256 GW (JCGx), 2011 WL 1661532, at *6 (C.D. Cal. Apr. 28, 2011).[4]

B. The Trespass to Chattels Claim

To establish trespass to chattels, plaintiffs must show that PulsePoint intentionally, and without justification or consent, physically interfered with the use and enjoyment of personal property in their possession, and that they were harmed thereby. Sch. of Visual Arts v. Kuprewicz, 3 Misc. 3d 278, 281, 771 N.Y.S.2d 804, 807 (Sup. Ct. N.Y. Cty. 2003); Chevron Corp. v. Donziger, 871 F. Supp. 2d 229, 258 (S.D.N.Y. 2012). Possessors of chattel, unlike possessors of land, are not protected from "harmless intermeddlings." Restatement (Second) of Torts § 218 cmt. e (1965). There must be a resulting harm to "the possessor's materially valuable interest in the physical condition, quality, or value of the chattel," or else the possessor must be "deprived of the use of the chattel for a substantial time" or have some

[4] We note that language in a parenthetical added to the CFAA as part of the USA PATRIOT Act of 2001, see Pub. L. No. 107-56, § 814(a), 115 Stat. 272, 383 (2001), suggests losses may not be aggregated among multiple computers for purposes of the $5,000 threshold in private suits. Factor (I) now refers to "loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States **only**, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value." 18 U.S.C. § 1030(c)(4)(A)(i)(I) (emphases added).

other legally protected interest in the property affected. Id.; see Kuprewicz, 3 Misc. 3d at 281, 771 N.Y.S.2d at 807-08 (adopting Restatement standard). For this reason, as applied to the online context, trespass "does not encompass . . . an electronic communication that neither damages the recipient computer system nor impairs its functioning." Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1347, 71 P.3d 296, 300 (2003); see id. at 1356, 71 P.3d at 306 ("In the decisions so far reviewed, the defendant's use of the plaintiff's computer system was held sufficient to support an action for trespass when it actually did, or threatened to, interfere with the intended functioning of the system, as by significantly reducing its available memory and processing power.").[5]

PulsePoint persuasively contends that plaintiffs have not alleged the necessary harm to sustain their trespass claim. As discussed in the Article III injury analysis, there are no particularized allegations of diminished device performance. At most, plaintiffs have plausibly alleged some unspecified increase in the use of device storage or processing capacity, without alleging that this uptick was significant or caused any discernible effect on the operation of their devices. As other courts have held based on similar allegations, plaintiffs must do more than

[5] California applies the standard of harm embodied in the Restatement. Hamidi, 30 Cal. 4th at 1351-52, 71 P.3d at 302-03.

simply claim an unspecified demand on their devices' resources to plausibly allege harm from trespass. See In re Google Android Consumer Privacy Litig., No. 11-MD-02264 JSW, 2013 WL 1283236, at *13 (N.D. Cal. Mar. 26, 2013) (dismissing trespass claim based on allegations that defendants installed unwanted code on phones to collect data and caused phone batteries to drain more quickly); iPhone Application Litig., 844 F. Supp. 2d at 1069 (allegations of consumption of "valuable bandwidth and storage space" and shortened battery life did "not plausibly establish a significant reduction in service constituting an interference with the intended functioning of the system"); LaCourt v. Specific Media, Inc., 2011 WL 1661532, at *7; cf. Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 980–81 (N.D. Cal. 2013) (denying motion to dismiss where plaintiff plausibly alleged defendant's use of its website "could divert sufficient computing and communications resources to impair the website's and servers' functionality").

The decisions cited by plaintiffs do not convince us to hold otherwise. In Register.com, Inc. v. Verio, Inc., the Court relied in part on the district court's finding that the defendant's use of search robots "consumed a significant portion of the capacity of [plaintiff's] computer systems," 356 F.3d 393, 404-05 (2d Cir. 2004), and in Kuprewicz, the defendant had allegedly sent "large volumes" of unwanted e-mails which "depleted hard disk space, drained processing power, and adversely affected other system

resources on [plaintiff's] computer system," 3 Misc. 3d at 281-82, 771 N.Y.S.2d at 808 (internal quotation marks omitted). Those cases, unlike this one, involved allegations or findings of activity that either had or threatened to have a significant effect on the capacity of computer systems.[6]

Plaintiffs also contend that the deprivation of the use of Safari's third-party cookie blocker is sufficient harm. However, plaintiffs cite no authority for the argument that we may view one feature of a particular software application as chattel for purposes of a trespass claim. Cf. Restatement (Second) of Torts § 216 (1965) (defining "person who is in 'possession of a chattel'" as "one who has physical control of the chattel with the intent to exercise such control on his own behalf, or on behalf of another"); Thyroff v. Nationwide Mut. Ins., 8 N.Y.3d 283, 292–93, 864 N.E.2d 1272, 1278 (2007) (concluding that "electronic records that were stored on a computer and were indistinguishable from printed documents" were "subject to a claim of conversion in New York," but "not consider[ing] whether any of the myriad other forms of

[6] Plaintiffs argue that if PulsePoint is not held liable, its competitors will be incentivized to copy its conduct, resulting in a "bombard[ment]" of tracking cookies. Pl. Opp. at 23. The basis for this argument is Register, in which the Second Circuit also partially relied on the district court's finding that permitting the defendant to continue using its search robots to perform queries on Register's database made it "'highly probable'" that the defendant's competitors "would devise similar programs to access Register's data, and that [Register's computer] system would be overtaxed and would crash," 356 F.3d at 404. This Court has not been presented with any allegations concerning others replicating PulsePoint's conduct going forward. Most notably, unlike in Register, there is no claim of an ongoing trespass, see supra note 1.

virtual information should be protected by the tort").

Many harmless electronic intrusions could potentially be recast as deprivations of a particular feature of an application meant to keep the electronic communication out. For example, the circumvention of a spam filter by junk e-mail could be characterized as depriving the user of his or her spam filter even if the junk e-mail had no effect whatever on the functionality of the user's e-mail service. We think such a holding would upset the principle that no action for trespass lies for harmless intermeddlings with chattel. As plaintiffs have provided no support for their narrow framing of their possessory interests, we decline to adopt it here.

C. The GBL § 349 Claim

To state a claim under GBL § 349, a plaintiff must prove that (1) the challenged act or practice was consumer-oriented, (2) it was deceptive or misleading in a material way, and (3) the plaintiff has been injured by reason thereof. Oswego Laborers' Local 214 Pension Fund v. Marine Midland Bank, N.A., 85 N.Y.2d 20, 25, 647 N.E.2d 741, 744 (1995). The statute requires "actual" harm distinct from the deceptive conduct, though it need not necessarily be pecuniary harm. Stutman v. Chem. Bank, 95 N.Y.2d 24, 29, 731 N.E.2d 608, 612 (2000). PulsePoint argues that plaintiffs have failed to allege facts showing that they suffered an injury cognizable under GBL § 349.

According to plaintiffs, the following injuries give rise to their GBL § 349 claim: "the degradation in value of their Devices (including the complete disabling of a key feature of their browsers); the violation of their privacy; and the theft and monetization of their personal data." Pl. Opp. at 14. For the reasons stated previously, plaintiffs have not pled injury based on the monetization of their data. Nor can we see how plaintiffs have pled any degradation in device value based solely on the placement of some indeterminate number of cookies. Furthermore, we do not believe New York courts would permit an intrusion insufficient to constitute a trespass to chattels to sustain a GBL § 349 claim instead, and thus conclude that the alleged deprivation of the use of the Safari third-party cookie blocker also fails to state the necessary injury.

Finally, we agree with PulsePoint that plaintiffs have not alleged a privacy harm actionable under GBL § 349. Plaintiffs argue that "it is a violation of plaintiffs' privacy rights to aggregate web browsing history." Pl. Opp. at 9 (emphasis in original). Importantly, however, they concede that there are no allegations that PulsePoint was able to link that information to specific persons, rather than to a particular browser and/or device. Nor do they claim any resulting embarrassment or distress suffered by either Naiman or Mount. Instead, plaintiffs allege only that surreptitiously collecting this information was a

"violation of their statutorily protected privacy rights." FAC ¶ 57.

However, plaintiffs do not identify any New York statute—or any New York state court decision—enshrining their right to privacy in anonymous (or perhaps pseudonymous) internet browsing history information. Instead, principally relying on two New York State Supreme Court decisions, plaintiffs appear to suggest that such a right is protected by GBL § 349 itself. Careful consideration of those decisions reveals that they provide plaintiffs little assistance.

First, in Anonymous v. CVS Corp., 188 Misc. 2d 616, 618, 728 N.Y.S.2d 333, 335 (Sup. Ct. N.Y. Cty. 2001), CVS allegedly maintained a program through which it purchased records containing prescription and other medical information from independent pharmacies ceasing to do business. It allegedly required participating pharmacies not to give advance notice to their customers prior to closing and transferring their records to CVS. Id. Plaintiff, diagnosed with HIV and AIDS, claimed he selected his local pharmacy based on an expectation of privacy, and learned only after his pharmacy had closed that his records had been transferred and had been incorporated into CVS's database, accessible by CVS pharmacies, CVS employees, and companies that contracted with CVS. Id. at 618-19, 728 N.Y.S.2d at 335-36.

In considering plaintiff's GBL § 349 claim against his

pharmacy and CVS, the Court explained that the disclosure of HIV and AIDS related information was restricted by statute. Further, it assumed without deciding that, due to the special characteristics of the pharmacist-customer relationship and the personal nature of "confidential medical information," defendants owed plaintiff a duty of confidentiality with respect to non-HIV and AIDS related information. Id. at 620-25, 728 N.Y.S.2d at 336-40.[7] Rejecting defendants' argument that no actionable injury had been alleged, the Court held that by failing to provide plaintiff with prior notice of the transfer of his records, defendants had "prevented plaintiff from exercising the right to take action to prevent or minimize the disclosure of his medical information." Id. at 625, 728 N.Y.S.2d at 340.

Second, in Meyerson v. Prime Realty Servs., LLC, 7 Misc. 3d 911, 912, 796 N.Y.S.2d 848, 850 (Sup. Ct. N.Y. Cty. 2005), the defendant landlord directed plaintiff to complete a form requiring her to disclose her Social Security number (or "SSN"). The form falsely indicated that plaintiff's failure to disclose her SSN would be grounds for eviction or non-renewal of her lease. Id. at

[7] The Court dismissed plaintiff's claim based on New York Public Health Law § 2782, which prohibits disclosure of "confidential HIV related information" obtained "in the course of providing any health or social service or pursuant to a release of confidential HIV related information." CVS, 188 Misc. 2d at 628-29, 728 N.Y.S.2d at 342-43 (quoting N.Y. Pub. Health § 2782(1) (2001)). Although plaintiff's HIV and AIDS related information fell within the statute's definition of "confidential HIV related information," the Court held that either it was not obtained "in the course of providing any health or social service" as defined under the statute or its disclosure fell within a statutory exemption. Id. at 629, 728 N.Y.S.2d at 342-43.

918, 796 N.Y.S.2d at 854. The Court canvassed the legal treatment of SSNs, cataloging various restrictions in statutes and case law on government agencies' ability to request and disseminate SSNs. Id. at 913-17, 796 N.Y.S.2d at 851-54 (citing, inter alia, 1974 Privacy Act, 5 U.S.C. § 552a, Driver's Privacy Protection Act of 1994, 18 U.S.C. §§ 2721-2725, and decisions holding that SSNs were confidential in response to freedom of information requests). Recognizing that "New York generally follows the same principles," it concluded that the "weight of authority favors treating a social security number as private and confidential information" that appears to be "protected by something akin to a privilege against disclosure." Id. at 917, 796 N.Y.S.2d at 853-54.

Turning to the GBL § 349 injury requirement, the Court held that plaintiff's allegations of anxiety, distress, and pre-litigation attorney's fees were sufficient. In addition, it "[could]not be doubted that a privacy invasion claim . . . may be stated under GBL § 349 based on non-pecuniary injury, such as deprivation of the right to maintain the privacy of medical records." Id. (citing CVS, 188 Misc. 2d 616, 728 N.Y.S.2d 333).

The claimed injury here does not fit comfortably within this precedent. To begin, while we acknowledge that the observation of an internet user's aggregated browsing history may reveal intimate details of that user's life, there are no allegations that plaintiffs' browsing histories were at risk of being de-anonymized

or used for any purpose other than targeted advertising. This suggests that this data, at least in the abstract, occupies a lower level in the hierarchy of sensitive information as compared to SSNs, the disclosure of which the Meyerson Court noted could increase the risk of identity theft, 7 Misc. 3d at 912–13, 796 N.Y.S.2d at 850–51, and medical records actually identifying individuals in addition to, among other things, their prescriptions, allergies, drug reactions, and chronic diseases, see CVS, 188 Misc. 2d at 618 & n.1, 728 N.Y.S.2d at 335 & n.1.

More importantly, both decisions treated the information at issue as presumptively confidential; linked the alleged right in preventing disclosure to statutes regulating the dissemination of such information; and assumed that maintaining its confidentiality in the circumstances presented was a right protected by an independent duty or privilege. Plaintiffs supply no basis for us to assume that New York courts would consider the information allegedly collected here to possess a similar status. Instead, they largely rely on out-of-state decisions considering whether alleged unauthorized collection of browsing information was sufficient to plead intrusion upon seclusion, see Nickelodeon, 2016 WL 3513782, at *23-25 (New Jersey common law intrusion claim); Google, 806 F.3d at 149-52 (California common law intrusion claim and privacy claim based on California Constitution); Ung v. Facebook, Inc., No. 1-12-CV-217244 (Cal. Super. Ct. Santa Clara

Cty. Jul. 2, 2012) (privacy claim based on California Constitution), but that cause of action is unavailable under New York law, see Howell v. New York Post Co., 81 N.Y.2d 115, 123, 612 N.E.2d 699, 703 (1993). Indeed, New York has no common-law right of privacy, and recognizes a right of action for invasion of privacy exclusively through New York Civil Rights Law §§ 50-51, which proscribe the unauthorized use of a person's likeness for advertising or trade purposes, see id., and have no application here.[8]

This distinction in legal context counsels more broadly in favor of caution before permitting GBL § 349 claims based on collection of information beyond those categories recognized in CVS and Meyerson. Cf. Valeriano v. Rome Sentinel Co., 43 A.D.3d 1357, 1358, 842 N.Y.S.2d 805, 806 (4th Dep't 2007) (failure to dismiss negligence claim based on publication of personal information where defendant had no duty to protect confidentiality of such information "would result in the 'circumvention of

[8] As PulsePoint notes, even plaintiffs with invasion of privacy causes of action based in state constitutions or common law at their disposal have not found uniform pleading success based on similar allegations. For example, in a decision cited by plaintiffs, the Santa Clara County Superior Court found a legally protected privacy interest in a Facebook user's "identifiable browsing history" because Facebook had the ability to link the data to the user's Facebook account; the Court, however, dismissed the claims of non-Facebook members because they did not "have any privacy right in their browsing data that has not been linked to their identities." Ung, No. 12-CV-217244, Order at *2-3; see also Yunker, 2013 WL 1282980, at *15 (allegations that mobile application provided identifiable personal information to advertisers in violation of its privacy policy did not rise to level of "egregious breach of social norms" so as to constitute violation of California's constitutional right to privacy).

established privacy law'" (brackets omitted) (quoting Madden v. Creative Servs., Inc., 84 N.Y.2d 738, 747, 646 N.E.2d 780, 785 (1995))). While not directly on point, we find Smith v. Chase Manhattan Bank, USA, N.A., 293 A.D.2d 598, 741 N.Y.S.2d 100 (2d Dep't 2002), instructive. There, a putative class brought GBL § 349 claims against defendants for violating their promise not to share customer information by disclosing customers' names, addresses, phone numbers, and financial data to third-party vendors who used the information for marketing. Id. at 598, 741 N.Y.S.2d at 101. In affirming dismissal, the Second Department found the allegations stated actionable deception, but not actionable injury: the harm at the "heart" of the complaint was that "class members were merely offered products and services which they were free to decline," and in the Court's view that did not suffice. Id. at 599, 741 N.Y.S.2d at 102. That Smith did not focus on the disclosure of the customers' data as the central harm further dissuades us from extension of CVS and Meyerson.

For all of these reasons, we find unpersuasive the contrary conclusion reached on this issue in Bose v. Interclick, Inc., No. 10 Civ. 9183, 2011 WL 4343517, at *1-2, *9 (S.D.N.Y. Aug. 17, 2011), which considered allegations of deceptive web monitoring through "flash cookies" and browser "history sniffing" code. In finding actual injury to have been sufficiently pled, Bose explained that courts "have recognized similar privacy violations

as injuries for purposes of Section 349," and cited to CVS and Meyerson. 2011 WL 4343517, at *9. As discussed, we believe those cases to be distinguishable, and, absent any New York decisions suggesting a privacy right in anonymized browsing history, decline to channel privacy claims based on its collection through GBL § 349.

Because we conclude that neither plaintiff can bring a GBL § 349 claim, we need not address PulsePoint's additional argument that Mount, domiciled in New Jersey, is not protected by the statute.

D. The Unjust Enrichment Claim

An unjust enrichment claim has three elements: first, the defendant was enriched; second, the enrichment was at the plaintiff's expense; and third, the defendant's retention of the benefit would be unjust. Kossoff v. Felderbaum, No. 14 Civ. 1144 (RWS), 2016 WL 1364290, at *3 (S.D.N.Y. Apr. 4, 2016). As plaintiffs concede, our conclusion that they have failed to plead injury based on misappropriation of the value of their browsing information requires dismissal of this claim. See Pl. Opp. at 12 (such injury provides "only basis for the unjust enrichment claim"); see also Edelman v. Starwood Capital Grp., LLC, 70 A.D.3d 246, 250, 892 N.Y.S.2d 37, 40 (1st Dep't 2009) (unjust enrichment claim failed where "alleged benefit to defendants" of using plaintiffs' proprietary information "did not come at plaintiffs'

expense, and plaintiffs did not suffer any loss in connection with that use for which restitution is an appropriate remedy").

CONCLUSION

For the foregoing reasons, PulsePoint's motion to dismiss the amended complaint pursuant to Rule 12(b)(1) is denied and its motion to dismiss the amended complaint pursuant to Rule 12(b)(6) is granted. The Clerk of the Court is respectfully directed to terminate the pending motion at ECF No. 29 and close the case.

DATED: New York, New York
August 17, 2016

NAOMI REICE BUCHWALD
UNITED STATES DISTRICT JUDGE