IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF DELAWARE

IN RE: GOOGLE INC. COOKIE PLACEMENT CONSUMER PRIVACY LITIGATION	)	MDL Civ. No. 12-2358-SLR

Charles Slanina, Esquire and David L. Finger, Esquire of Finger & Slanina, LLC, Wilmington, Delaware. Liaison Counsel for Plaintiffs. Plaintiffs' Lead Counsel: Stephen G. Grygiel, Esquire of Keefe Bartels, LLC, James Frickleton, Esquire of Bartimus, Frickleton, Robertson & Gorny, P.C., and Brian Russell Strange, Esquire of Strange & Carpenter. Plaintiffs' Steering Committee: David Straite, Esquire of Kaplan, Fox & Klischeimer, L.L.P., Jonathan Shub, Esquire of Seeger Weiss LLP, Barry Eichen, Esquire of Eichen, Crutchlow, Zaslow & McElroy, LLP, William "Billy" Murphy, Esquire of Murphy, P.A., Mark Bryant, Esquire of The Bryant Law Center, PSC, and, Jay Barnes, Esquire of Barnes & Associates.

Michael H. Rubin, Esquire, Anthony J. Weibell, Esquire, and C. Scott Andrews, Esquire of Wilson Sonsini Goodrich & Rosati. Counsel for Defendant Google.

Susan M. Coletti, Esquire of Fish & Richardson P.C., Wilmington, Delaware. Counsel for Defendant PointRoll, Inc. Of Counsel: Alan Charles Raul, Esquire and Edward R. McNicholas, Esquire of Sidley Austin LLP.

Kelly E. Farnan, Esquire, Rudolf Koch, Esquire, and Travis S. Hunter, Esquire of Richards, Layton & Finger, Wilmington, Delaware. Counsel for Defendant Vibrant Media Inc. Of Counsel: Edward P. Boyle, Esquire, David N. Dinotti, Esquire, and Joeann E. Walker, Esquire of Venable LLP.

Rodger D. Smith II, Esquire and Regina S.E. Murphy, Esquire of Morris, Nichols, Arsht & Tunnell LLP, Wilmington, Delaware. Counsel for Defendants Media Innovation Group, LLC and WPP plc. Of Counsel: Douglas H. Meal, Esquire and Lisa M. Coyle, Esquire of Ropes & Gray LLP.

MEMORANDUM OPINION

Dated: October 9, 2013
Wilmington, Delaware

ROBINSON, District Judge

I. INTRODUCTION

On December 19, 2012, four named plaintiffs ("plaintiffs") filed a consolidated amended complaint ("CAC") in this multidistrict consolidated litigation against Google Inc. ("Google"), Vibrant Media, Inc. ("Vibrant"), Media Innovation Group LLC ("Media"), and WPP, plc ("WPP"), (collectively "defendants"), as well as PointRoll, Inc.[1] (D.I. 46) On July 23, 2013, plaintiffs settled with PointRoll, Inc. (D.I. 109) Plaintiffs allege that defendants "tricked" their Apple Safari ("Safari") and/or Internet Explorer ("IE") browsers into accepting cookies, which then allowed defendants to display targeted advertising.

Pending before the court are three motions to dismiss: Google's motion to dismiss the consolidated amended complaint (D.I. 56); Vibrant's motion to dismiss for failure to state a claim (D.I. 93); and Media and WPP's motion to dismiss for failure to state a claim (D.I. 96). The court has jurisdiction pursuant to 28 U.S.C. § 1331 and 28 U.S.C. § 1332(d), and supplemental jurisdiction over the state law claims under 28 U.S.C. § 1367.

II. BACKGROUND

A. Parties

Google is a Delaware corporation with its headquarters at 1600 Amphitheatre Parkway, Mountain View, CA 94043. Google is a technology leader and also delivers relevant, cost-effective online advertising. (D.I. 46 at ¶¶ 14,19) Vibrant is a Delaware corporation, headquartered in New York, New York. Vibrant is known for its in-text ads,

---

[1]The Judicial Panel on Multidistrict Litigation has centralized these actions in this district for consolidated pretrial proceedings pursuant to 28 U.S.C. § 1407. (D.I. 1) There are 25 individual cases. Unless otherwise noted, all citations are made to the record of Civ. No. 12-2358.

which pop up in the text of articles on the web. (D.I. 46 at ¶¶ 16, 24) Media is a Delaware limited liability company headquartered in New York, New York. Media provides targeted online advertising. (D.I. 46 at ¶¶ 17, 25) WPP, a public limited company with its main offices in Dublin, Ireland, and London, United Kingdom, owns Media and describes itself as "the world leader in marketing communications services." (D.I. 46 at ¶¶ 18, 26)

B. Factual Background

Internet "cookies" are used to track an individual's activities and communications on a particular website and across the internet.[2] Cookies are used in internet advertising to store website preferences, retain the contents of shopping carts between visits, and keep browsers logged into social networking services and webmail as individuals surf the internet. "First-party cookies" are set by the website the user is visiting at the time the cookie is set. "Third-party cookies" are placed on a user's device by a website other than the site the user is visiting at the time the cookie is set. (D.I. 46 at ¶¶ 38-39, 45-46) "[T]hird-party cookies are used by advertising companies to help create detailed profiles on individuals, including, but not limited to an individual's unique ID number, IP address, browser, screen resolution, and a history of all websites visited within the ad network by recording every communication request by that browser to sites that are participating in the ad network, including all search terms the user has entered. The information is sent to the companies and associated with unique cookies -- that is how the tracking takes place." (*Id.* at ¶ 46)

---

[2]All facts are taken from the CAC.

"Every document has a unique 'URL' (Universal Resource Locator) that identifies its physical location in the Internet's infrastructure." (D.I. 46 at ¶ 10 n.1) When a user requests a website, "the user's Safari browser starts by sending a GET request to the server which hosts the publisher's webpage," to retrieve the data for display on the user's monitor. (*Id.* at ¶ 85) Many websites will leave part of their webpage blank for third-party companies to insert advertisements. Upon receiving a GET request from a user seeking to display a particular webpage, the server for that webpage will respond to the browser, instructing the browser to send a GET request to the third-party company charged with serving the advertisements for that particular webpage. The third party receives the GET request and a copy of the user's request to the first-party website and responds by sending the advertisement to the user's browser which displays it on the user's device. (*Id.* at ¶ 41)

Defendants used coding in advertisements to circumvent Apple's Safari browser's default blocker and deceive the IE browser into accepting third-party cookies. (D.I. 46 at ¶¶ 68-190) Google stopped only when caught and began removing the illicit cookies. (*Id.* at ¶ 119) If users are logged-in to a Google account, Google is then able "to synchronize the ads with the particular user's personalized information," allowing for targeted advertising. (*Id.* at ¶ 89) This information includes the information provided by the user, defined by Google to include "information which you provide to us which personally identifies you, such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google," as well as address information and browsing history information. (*Id.* at ¶ 98) One of the third-

party cookies set by defendants assigned a unique ID to the user's computing device which allowed defendants to associate future information received to the unique ID. (*Id.* at ¶¶ 78, 95, 150, 153-54)

III. ARTICLE III STANDING

Article III standing requires: "(1) an injury-in-fact . . . ; (2) a causal connection between the injury and the conduct complained of; and (3) that it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Winer Family Trust v. Queen*, 503 F.3d 319, 325 (3d Cir. 2007). To have standing, "the 'injury in fact' test requires more than an injury to a cognizable interest. It requires that the party seeking review be himself among the injured." *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992) (quoting *Sierra Club v. Morton*, 405 U.S. 734, 734-735 (1972)). "The actual or threatened injury required by Art. III may exist solely by virtue of 'statutes creating legal rights, the invasion of which creates standing . . . ." *See Warth v. Seldin*, 422 U.S. 490, 500 (1975) (citing *Linda R.S. v. Richard D.*, 410 U.S. 614, 617 n. 3 (1973)).

Plaintiffs cite to many articles to support their allegations that personally identifiable information ("PII") has monetary value and is a commodity that companies trade and sell. (D.I. 46 at ¶¶ 49-67) Specifically, "[t]he cash value of users' personal information can be quantified," with web browsing histories valued at $52 per year. (*Id.* at ¶ 56) Plaintiffs also describe a company which calculates the value of a user's web activity. (*Id.* at ¶ 66) Google offers users the opportunity to join a panel which allows Google to track the websites the user visits in exchange for gifts, such as gift cards to

retailers. (*Id.* at ¶¶ 57-60) Plaintiffs describe a company in the United Kingdom which offers users a real market for their personal information and a start-up company which "enables people to sell themselves to advertisers directly," valuing user's data at $12 per year. (*Id.* at ¶¶ 63-64)

District courts have been reluctant to equate loss of PII, without more, to injury in fact. For instance, in *LaCourt v. Specific Media, Inc.*, No. 10-1256, 2011 WL 1661532 (C.D. Cal. Apr. 28, 2011), plaintiffs alleged that

> they "are persons who have set the privacy and security controls on their browsers to block third-party cookies and/or who periodically delete third-party cookies," and that they each had a "Flash cookie" installed on their computer by Specific Media without their notice or consent.
> Plaintiffs allege that they sought to maintain the secrecy and confidentiality of the information obtained by Defendant through the use of [local shared objects]. They further allege that "Defendant's conduct has caused economic loss to Plaintiffs and Class Members in that their personal information has discernable value, both to Defendant and to Plaintiffs and Class Members, and of which Defendant has deprived Plaintiffs and Class Members and, in addition, retained and used for its own economic benefit."

Id. at *2. The district court found that plaintiffs did not "explain how they were 'deprived' of the economic value of their personal information simply because their unspecified personal information was purportedly collected by a third party" and, therefore, did not have standing. *Id.* at *6; *see also, Del Vecchio v. Amazon.com Inc.*, No. 11-366, 2011 WL 6325910, at *3 (W.D. Wash. Dec. 1, 2011) ("*Del Vecchio I*") (the theoretical possibility that plaintiffs' information could lose value as a result of its collection and use by defendant was not enough for the court to reasonably infer that such devaluation had actually occurred). In contrast, the court in *Del Vecchio v. Amazon.com, Inc.*, No.

11-366, 2012 WL 1997697 (W.D. Wash. June 1, 2012) ("*Del Vecchio II*") found that plaintiffs alleged sufficient injury to have standing when they alleged "the dissemination and use of personal information belonging to them, including sensitive information about their web browsing and shopping habits, purchases, and related transaction information, **combined with** their financial information such as credit and debit card information, and their mailing and billing addresses." *Id.* at *2 (emphasis added). In *Claridge v. RockYou*, 785 F. Supp. 2d 855 (N.D. Cal. 2011), plaintiff alleged that defendant failed "to secure and safeguard its users' sensitive personally identifiable information . . . , including email addresses, passwords, and login credentials for social networks like MySpace and Facebook." *Id.* at 858. The district court doubted "plaintiff's ultimate ability to prove his damages theory," but found "plaintiff's allegations of harm sufficient at [the pleading] stage to allege a generalized injury in fact." *Id.* at 861.

In the case at bar, the CAC details that online personal information has value to third-party companies and is a commodity that these companies trade and sell. (D.I. 46 at ¶¶ 49-67) Examining the facts alleged in the light most favorable to plaintiffs, the court concludes that, while plaintiffs have offered some evidence that the online personal information at issue[3] has some modicum of identifiable value to an individual plaintiff, plaintiffs have not sufficiently alleged that the ability to monetize their PII has

[3]As identified by plaintiffs, a copy of the user's request to the first-party website (D.I. 46 at ¶ 41). If users are logged-in to a Google account, this information may also be matched up to information provided by the user, defined by Google to include "information which you provide to us which personally identifies you, such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google," as well as address information and browsing history information. (*Id.* at ¶¶ 89, 98)

been diminished or lost by virtue of Google's previous collection of it.

For the above reasons, the court concludes that plaintiffs have not alleged injury-in-fact sufficient to confer Article III standing. However, because a statutory violation, in the absence of any actual injury, may in some circumstances create standing under Article III, the court will address whether plaintiffs have pled sufficient facts to establish a plausible invasion of the rights created by the various statutes asserted. *Alston v. Countrywide Financial Corp.*, 585 F.3d 753, 763 (3d Cir. 2009).

IV. MOTION TO DISMISS

A. Standard of Review

A motion filed under Federal Rule of Civil Procedure 12(b)(6) tests the sufficiency of a complaint's factual allegations. *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555; *Kost v. Kozakiewicz*, 1 F.3d 176, 183 (3d Cir. 1993). A complaint must contain "a short and plain statement of the claim showing that the pleader is entitled to relief, in order to give the defendant fair notice of what the . . . claim is and the grounds upon which it rests." *Twombly*, 550 U.S. at 545 (internal quotation marks omitted) (interpreting Fed. R. Civ. P. 8(a)). Consistent with the Supreme Court's rulings in *Twombly* and *Ashcroft v. Iqbal*, 556 U.S. 662 (2009), the Third Circuit requires a two-part analysis when reviewing a Rule 12(b)(6) motion. *Edwards v. A.H. Cornell & Son, Inc.*, 610 F.3d 217, 219 (3d Cir. 2010); *Fowler v. UPMC Shadyside*, 578 F.3d 203, 210 (3d Cir. 2009). First, a court should separate the factual and legal elements of a claim, accepting the facts and disregarding the legal conclusions. *Fowler*, 578 F.3d. at 210-11. Second, a court should determine whether the remaining well-pled facts sufficiently

show that the plaintiff "has a 'plausible claim for relief.'" *Id.* at 211 (quoting *Iqbal*, 556 U.S. at 679). As part of the analysis, a court must accept all well-pleaded factual allegations in the complaint as true, and view them in the light most favorable to the plaintiff. *See Erickson v. Pardus*, 551 U.S. 89, 94 (2007); *Christopher v. Harbury*, 536 U.S. 403, 406 (2002); *Phillips v. Cnty. of Allegheny*, 515 F.3d 224, 231 (3d Cir. 2008). In this regard, a court may consider the pleadings, public record, orders, exhibits attached to the complaint, and documents incorporated into the complaint by reference. *Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007); *Oshiver v. Levin, Fishbein, Sedran & Berman*, 38 F.3d 1380, 1384-85 n.2 (3d Cir. 1994).

The court's determination is not whether the non-moving party "will ultimately prevail" but whether that party is "entitled to offer evidence to support the claims." *United States ex rel. Wilkins v. United Health Grp., Inc.*, 659 F.3d 295, 302 (3d Cir. 2011). This "does not impose a probability requirement at the pleading stage," but instead "simply calls for enough facts to raise a reasonable expectation that discovery will reveal evidence of [the necessary element]." *Phillips*, 515 F.3d at 234 (quoting *Twombly*, 550 U.S. at 556). The court's analysis is a context-specific task requiring the court "to draw on its judicial experience and common sense." *Iqbal*, 556 U.S. at 663-64.

B. The Electronic Communications Privacy Act[4]

The Electronic Communications Privacy Act ("the Wiretap Act") protects "any person whose wire, oral, or electronic communication is intercepted, disclosed, or

[4]Count I, against all defendants.

intentionally used in violation of this chapter . . . ." 18 U.S.C. 2520(a). It imposes liability on a person who "intentionally intercepts" and discloses the "contents" of an "electronic communication," 18 U.S.C. § 2511(1)(a), (c); § 2510(4), unless "such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception . . . ." 18 U.S.C. § 2511(2)(d). "'[C]ontents,' when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication." 18 U.S.C. § 2510(8). "Contents" is information the user intended to communicate, such as the spoken words of a telephone call. *United States v. Reed*, 575 F.3d 900, 916 (9th Cir. 2009).

Based on plaintiffs' factual allegations, plaintiffs' browsers voluntarily sent to Google the information inputted by plaintiffs, regardless of whether plaintiffs' browsers had any Google cookies set. Because of this, Google is plausibly a party to the communications. However, as defendants bypassed the browser settings to place cookies that would allow them to later associate plaintiffs' data, the court declines to characterize defendants as within the statutory "party" exception. Moreover, viewing the facts in the light most favorable to plaintiffs, plaintiffs' browsers sent different information in response to targeted advertising than would have been sent without the setting of third-party cookies. For this reason also, Google is not appropriately deemed a party to the communications.

Plaintiffs argue that defendants intercepted both transactional information and "contents," such as the URLs and "information that Class Members exchanged with first-party websites during the course of filling out forms or conducting searches." (D.I.

81 at 17) Most of this information cannot be characterized as "contents." Specifically, "personally identifiable information that is automatically generated by the communication" is not "contents" for the purposes of the Wiretap Act. *See, e.g., In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1062 (2012) ("*iPhone II*") (data conveying the geolocation of plaintiffs was not contents, as it was automatically generated by the iPhone); *Sams v. Yahoo!, Inc.*, No. 10-5897, 2011 WL 1884633, at *6-7 (N.D. Cal. May 18, 2011) (records identifying persons using Yahoo ID and email address, IP addresses, and login times was not content-based); *In re § 2703(d) Order*, 787 F. Supp. 2d 430, 435-36 (E.D. Va. 2011) (the Wiretap Act did not cover unique Internet Protocol ("IP") number, Twitter subscriber, user, and screen names, addresses (including e-mail addresses), telephone or instrument number or other subscriber number or identity, and temporarily assigned network address).

With respect to URLs, it is important to note that plaintiffs' browsers would send a URL regardless of whether a third party cookie was set. To date, no courts have characterized URLs as "contents" for the purposes of the Wiretap Act.[5] *U.S. v. Allen*,

---

[5]In the context of a Fourth Amendment analysis and in dicta, the United States Court of Appeals for the Ninth Circuit did note its concern over unauthorized access to URLs:

> "[s]urveillance techniques that enable the government to determine not only the IP addresses that a person accesses but also the [URL] of the pages visited might be more constitutionally problematic. A URL, unlike an IP address, identifies the particular document within a website that a person views and thus reveals much more information about the person's Internet activity. For instance, a surveillance technique that captures IP addresses would show only that a person visited the New York Times' website at http://www.nytimes.com, whereas a technique that captures

53 M.J. 402, 409 (C.A.A.F. 2000) ("log identifying the date, time, user, and detailed internet address of sites accessed by appellant over several months" was "transactional records" for purposes of the Wiretap Act); *see also U.S. v. Polizzi*, 549 F. Supp. 2d 308, 393 (E.D.N.Y. 2008) (finding in the context of a Fourth Amendment search that "[n]o expectation of privacy exists for other . . . online transactional information, such as a user's Internet search history"), vacated on other grounds by 564 F.3d 142 (2d Cir. 2009). As described by their name, "Universal Resource Locators," URLs do not change and are used to identify the physical location of documents in the internet's infrastructure. While URLs may provide a description of the contents of a document, e.g., www.helpfordrunks.com, a URL is a location identifier and does not "concern[] the substance, purport, or meaning" of an electronic communication. 18 U.S.C. § 2510(8). Even if plaintiffs' browsers were "tricked" into sending the URLs to Google, the court concludes that Google did not intercept contents as provided for by the Wiretap Act. Given this legal obstacle, defendants' motions to dismiss are granted.

C. The California Invasion of Privacy Act[6]

To prevail on their claim under the California Invasion of Privacy Act, Penal Code § 630, et seq. (the "CIPA"), plaintiffs would have to demonstrate that Google "willfully and without the consent of all parties to the communication, or in any unauthorized

---

> URLs would also divulge the particular articles the person viewed."

U.S. v. Forrester, 512 F.3d 500, 510 n.6 (9th Cir. 2008) (looking at surveillance of a specific person). The Court concluded that the surveillance at issue did not constitute a Fourth Amendment search and seizure. *Id.* at 510-11.

[6]Count VIII, against Google.

manner," intercepted, used, or disclosed the "contents or meaning" of a "communication" that is "in transit." 14 Cal. Pen. Code § 631(a)); CAC ¶ 266.

As with the Wiretap Act claim above, the court concludes that Google would have received the inputted information, including the URL, regardless of the setting of third-party cookies. Further, plaintiffs' allegations do not demonstrate that Google intercepted any "contents or meaning." For these reasons, Google's motion to dismiss is granted.

D. The Stored Communications Act[7]

The Stored Communications Act ("SCA"), 18 U.S.C. § 2701 et seq., renders liable whoever "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system . . . ." 18 U.S.C. § 2701(a). The general prohibitions under § 2701(a) do not apply "to conduct authorized (1) by the person or entity providing a wire or electronic communications service; [or] (2) by a user of that service with respect to a communication of or intended for that user." 18 U.S.C. § 2701(c).

In enacting the SCA, Congress was concerned that the Fourth Amendment may not protect against searches and seizures of copies of electronic communications stored by third parties. *See* S. Rep. No. 99-541 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3557, 1986 WL 31920, at *3 ("[P]roviders of electronic mail create electronic

---

[7]Count II, against all defendants.

copies of private correspondence for later reference . . . For the person or business whose records are involved, the privacy or proprietary interest in that information should not change. Nevertheless, because it is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection."); *see also Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 900 (9th Cir. 2008) ("The SCA was enacted because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address."). The SCA fills that constitutional gap by protecting against unauthorized access to electronic communications in third-party hands, e.g., internet service providers.

Certainly the technological landscape today is much different than it was in 1986, when the SCA was enacted. Along with the changes in technology have come different privacy concerns, as illustrated by the instant litigation. The question framed by the pending motion is whether the language of the SCA can be interpreted broadly enough, consistent with the rules of statutory interpretation, to accommodate the evolving technology.

Statutory interpretation begins with the plain language of the statute. *See Jimenez v. Quarterman*, 555 U.S. 113, 118 (2009) ("As with any question of statutory interpretation, our analysis begins with the plain language of the statute."). The Third Circuit has instructed courts to consider "'not only the particular statutory language at issue, but also the structure of the section in which the key language is found, the design of the statute as a whole and its object.'" *Register v. PNC Financial Servs. Group, Inc.*, 477 F.3d 56, 67 (3d Cir. 2007) (quoting *Alaka v. Attorney General*, 456

F.3d 88, 104 (3d Cir. 2006)). In this regard, "'[s]tatutes should be interpreted to avoid untenable distinctions and unreasonable results whenever possible.'" *Id.* (quoting *American Tobacco Co. v. Patterson*, 456 U.S. 63, 71 (1982)).

Of the courts that have found it appropriate to apply the language of the SCA in a contemporary context, the analysis of the court in *Cousineau v. Microsoft Corp.*, Case No. C11-1438-JCC (W.D. Wash. June 22, 2012) (D.I. 81, ex. A), is the most persuasive, but only to a point. More specifically, in addressing the meaning of "facility" in § 2701(a) (a term left undefined by Congress), the court observed that

> Congress chose a broad term - facility - where it intended the statute to cover a particular function, such as internet access, as opposed to a particular piece of equipment providing that access, such as a router, laptop or smart phone. As technology evolves, identifying a smart phone as a facility through which an [electronic communication service or] ECS is provided is not as "strained" as it once may have seemed. . . . While earlier stages of technological development may have required large facilities for data storage, the draw of mobile devices is that their smaller storage space enables communication and information access regardless of the user's location.

Id. at 10-11. In concluding that "a mobile device can be a facility for the purposes of the SCA" (*id.*), the court further reasoned that "[a] chief purpose of smart phones is to 'promote the ease' of actions such as navigating from place to place, sharing information with others, and capturing images," all consistent with the dictionary definition of "facility," that is, "'something that promotes the ease of any action, operation, transaction or course of conduct.'" *Id.*

The problem with embracing this expanded notion of the term "facility," however, is that it confounds the distinction between "users" and "providers" which, in turn,

realigns the targeted conduct and makes the statutory exceptions found in § 2701(c) nonsensical. With respect to the legislative history of the SCA as related above, there can be no dispute that the individual owners of personal computers were the "users" contemplated under the statute and that the "providers" of the "electronic communication services" were contemplated to be third parties. As explained by the court in *iPhone II,* if now the "facility" is an individual's own personal computer that "provides" the electronic communication service, then

> the web site is a "user" of the communication service provided by the individual's computer, and consequently any communication between the individual computer and the web site is a communication "of or intended for" that web site, triggering the § 2701(c)(2) exception for authorized access. Likewise here, if plaintiffs' iPhones were the facilities, then any app downloaded by a plaintiff would be a "user" of that service for whom the iPhone's communications are intended; any communication between the iPhone and the app would be of or intended for that app; and the app developers would then be free under § 2701(c)(2) to authorize the disclosure of such communication to the Mobile Industry Defendants.

844 F. Supp. 2d at 1058. *See also, Crowley v. CyberSource Corp.,* 166 F. Supp. 2d 1263, 1270-71 (N.D. Cal. 2001); *Chance v. Ave. A., Inc.*, 165 F. Supp. 2d 1153, 1161 (W.D. Wash. 2001).

Despite the temptation, the court declines to try to fit a square peg (modern technology) into the proverbial round hole (the intent of Congress as reflected in the statutory language of the SCA). An individual's personal computing device is not "a facility through which an electronic communication service is provided," as required under the SCA.

Nevertheless, for purposes of completing this analysis, the court addresses

whether plaintiffs have sufficiently alleged that the electronic communications at issue were in "electronic storage" in a facility. 18 U.S.C. § 2701(a). The SCA defines "electronic storage" as "(a) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (b) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2501(17). Plaintiffs at bar have pled that the third-party cookies were "placed," "set," or "loaded" on a user's device and stored in browser-managed files on plaintiffs' computers. (D.I. 46 at ¶¶ 39, 94, 217) Plaintiffs also allege that "the cookies . . . are updated regularly to record users' browsing activities as they happen." (*Id.* at ¶ 218) According to plaintiffs, defendants "acquired both recently updated cookies and related just-transmitted electronic communications out of random access memory . . . . The defendants[, therefore,] acquired those cookies and related electronic communications out of electronic storage, incidental to the transmission thereof." (*Id.;* D.I. 81 at 21-22)

The court understands that there is a difference between storage of electronic communications in browser-managed files stored on a computer's hard drive, and storage of electronic communications in the random access memory ("RAM") of a computer, with only the latter arguably satisfying the statutory requirement for "temporary, intermediate storage." There seems to be a consensus that "[t]he cookies' long-term residence on plaintiffs' hard drives places them outside of § 2510(17)'s definition of 'electronic storage' and, hence, [the SCA's] protection." *In re DoubleClick, Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 511-12 (S.D.N.Y. 2001); *see also, iPhone II*, 844 F. Supp. 2d at 1059; *In re Toys R Us, Inc. Privacy Litig.*, Civ. No. 00-2746, 2001

WL 34517252, at *3 (N.D. Cal. Oct. 9, 2001). Unlike the facts presented in the above cited cases, however, plaintiffs at bar have also alleged that "defendants' access occurred while the cookies were in RAM, rather than on the hard drive." *iPhone II*, 844 F. Supp. 2d at 1059; *see also, In re Toys R Us, Inc. Privacy Litig.*, 2001 WL 34517252, at *3.

In conclusion, although plaintiffs have satisfied their pleading requirement as to "electronic storage,"[8] plaintiffs' allegations fail to meet the "facility through which an electronic communication service is provided" requirement of the SCA. Therefore, defendants' motion to dismiss this cause of action is granted.

E. The Computer Fraud and Abuse Act[9]

The Computer Fraud and Abuse Act (CFAA) is primarily a criminal statute, intended to protect against traditional computer hacking. *P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504, 510 (3d Cir. 2005). Nonetheless, it provides a civil remedy to "[a]ny person who suffers damage or loss by reason of a violation of this section . . . ." 18 U.S.C. § 1030(g); *P.C. Yonkers*, 428 F.3d at 510-512. The CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). "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

---

[8]The issue of whether the third-party cookies were accessed in a computer's RAM or in its hard drive would be an issue of fact to be vetted through discovery.

[9]Count III, against all defendants.

other consequential damages incurred because of interruption of service." 18 U.S.C. § 1030(e)(11). The CFAA also requires that the defendants' action caused economic damages in excess of $5,000 over a one-year period. § 1030(a)(5)(B)(I).

Plaintiffs have not alleged the kind of damage or loss required to maintain a CFAA claim. More specifically, plaintiffs have not identified any impairment of the performance or functioning of their computers.[10] Generally, courts have rejected the contention that the unauthorized collection, use, or disclosure of personal information constitutes economic damages for the purposes of the CFAA. *iPhone II*, 844 F. Supp. 2d at 1066-68 (citations omitted); *In re DoubleClick*, 154 F. Supp. 2d at 525-26 (citations omitted). As discussed above under the Article III standing analysis, plaintiffs have not shown individual economic loss. *See Del Vecchio II*, 2012 WL 1997697, at *4 (regardless of whether plaintiffs' information has value to defendants, "the term 'loss' requires that [p]laintiffs suffer a detriment – a detriment amounting to more than $5,000."). Therefore, the court concludes that plaintiffs have not sufficiently alleged the threshold loss of $5,000 required by the CFAA.[11] Defendants' motion to dismiss this

---

[10]Plaintiffs' undeveloped argument - "Google's impairing the integrity of [p]laintiffs' browser 'system' through illicit cookies and of [p]laintiffs' 'data' or 'information' through unpermitted capture and use underscores [p]laintiffs' statutory 'damage'" - is not supported by the facts alleged in the CAC and does not identify the kind of loss or damage defined by the CFAA. (D.I. 81 at 24)

[11]The court does not view "Google's intentional circumvention of Safari and IE [as] each a 'single act' permitting aggregation of damages," as suggested by plaintiffs. Instead, the facts alleged in the CAC suggest multiple acts by multiple defendants. The acts occurred at different times and to different plaintiffs. As such, plaintiffs cannot aggregate their alleged damages. *In re iPhone Application Litig.*, No. 11-02250, 2011 WL 4403963, at *11 (N.D. Cal., Sept. 20, 2011) ("*iPhone I*") (citing *In re Toys R Us*, 2001 WL 34517252, at *11) (plaintiffs may aggregate individual damages to meet the damages threshold if the violation can be described as "one act.").

claim is granted.

F. The California Computer Crime Law[12]

The California Computer Crime Law ("CCL") prohibits "tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Pen. Code § 502(a). Only someone "who suffers damage or loss by reason of a violation" may bring a civil action under the law. *Id.* § 502(e). Each subsection of the CCL asserted by plaintiffs, with the exception of § 502(c)(8), requires a showing that Google acted "without permission." *Id.* § 502(c)(1), (2), (6), (7). Courts have interpreted acting "without permission" under § 502 as "accessing or using a computer, computer network, or website in a manner that overcomes technical or code-based barriers." *Facebook, Inc. v. Power Ventures, Inc.*, No. C08–05780, 2010 WL 3291750, at *11 (N.D. Cal. July 20, 2010); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 715-16 (N.D. Cal. 2011). Section 502(c)(8) creates liability for any person who "knowingly introduces any computer contaminant[13] into any computer,

---

[12]Count VII, against Google.

[13]The term "computer contaminant" is defined as follows:

> ... any set of computer instructions that are designed to modify, damage, destroy, record, or transmit information within a computer, computer system, or computer network without the intent or permission of the owner of the information. They include, but are not limited to, a group of computer instructions commonly called viruses or worms, that are self-replicating or self-propagating and are designed to contaminate other computer programs or computer data, consume computer resources, modify, destroy, record, or transmit data, or in some other fashion usurp the normal operation of the computer, computer system, or computer network.

computer system, or computer network." Cal. Penal Code § 502(c)(8).

As discussed in the analysis of Article III standing, plaintiffs have not sufficiently alleged damage or loss. Further, plaintiffs fail to sufficiently meet the "without permission" element of § 502. In this regard, plaintiffs allege that Safari's default settings provide an exception to the third-party cookie blocking for situations where a user submits a form to the third-party's website servers. Google exploited this exception by adding coding to ads, such that Safari believed the exception to be satisfied and that the user had submitted a form to Google. In doing so, Google exploited a standard Safari browser function. Although Google's actions may be objectionable, Google did not access plaintiffs' browsers by "overcom[ing] technical or code-based barriers." Nor did Google introduce a "contaminant" to "usurp the normal operation" of plaintiffs' browsers. The method of Google's exploitation of a normal function of plaintiffs' browsers is not in dispute and does not meet the requirements of the statute; therefore, Google's motion to dismiss this count is granted.

G. The California Constitution[14]

An invasion of privacy in violation of the California Constitution requires plaintiffs to show "(1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) conduct by defendant constituting a serious invasion of privacy." *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 35-37 (1994). These elements are used to "weed out claims that involve so insignificant or de minimis an

---

Cal. Pen. Code § 502(b)(10).

[14]Counts IV and V, against Google.

intrusion on a constitutionally protected privacy interest as not even to require an explanation or justification by the defendant." *Loder v. City of Glendale*, 14 Cal. 4th 846, 893 (1997). "Actionable invasions of privacy must be sufficiently serious in their nature, scope, and actual or potential impact to constitute an egregious breach of the social norms underlying the privacy right." *Hill*, 7 Cal. 4th at 38 (rules requiring college football players to submit to drug testing was not an egregious breach of social norms).

Even if plaintiffs could succeed in meeting the first two elements, the third element proves fatal to their claim. The transfer of inputted information[15] (which would have occurred regardless of Google's placement of cookies) does not rise to the level of a serious invasion of privacy or an egregious breach of social norms. *iPhone II*, 844 F. Supp. 2d at 1063 (transfer of plaintiffs' geolocation information, personal data and unique device identifier number was not an egregious breach of social norms). Neither is Google's subsequent association of multiple instances of plaintiffs' inputted information with other personal information to provide targeted advertising a sufficiently serious invasion of privacy. *See, e.g., London v. New Albertson's, Inc.*, No. 08-1173, 2008 WL 4492642, at *8 (S.D. Cal. Sept. 30, 2008) (no protected privacy interest in preventing pharmacy from correlating consumers' anonymous drug prescription information). Therefore, Google's motion to dismiss this count is granted.

---

[15]E.g., a copy of the user's request to the first-party website (D.I. 46 at ¶ 41). If users are logged-in to a Google account, this information may also be matched up to the information provided by the user, defined by Google to include "information which you provide to us which personally identifies you, such as your name, email address or billing information, or other data which can be reasonably linked to such information by Google," as well as address information and browsing history information. (*Id.* at ¶¶ 89, 98)

H. The California Unfair Competition Law[16]

The California Unfair Competition Law ("UCL") protects against business practices that are "unlawful, unfair or fraudulent." Cal. Bus. & Prof. Code § 17200. A private plaintiff needs to have "suffered injury in fact and ... lost money or property as a result of the unfair competition." *Id.* § 17204; *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 330 (2011) (to establish standing, a plaintiff must demonstrate a personal loss of money or property attributable to their own reasonable reliance on the allegedly unlawful business practices). The "lost money or property" requires that "a plaintiff . . . demonstrate some form of economic injury." *Kwikset*, 51 Cal. 4th at 323.

As discussed above, plaintiffs have not articulated an injury in fact sufficient for Article III standing. Similarly, plaintiffs have not shown a loss of money or property from Google's actions sufficient to confer standing under the UCL. *See e.g., Facebook*, 791 F. Supp. 2d at 714 (plaintiffs could not maintain a cause of action under the UCL alleging that defendant unlawfully shared their "personally identifiable information" with third-party advertisers); *iPhone I*, 2011 WL 4403963, at *14 (finding that plaintiffs' allegations of loss of personal information was insufficient for Article III standing and to maintain a cause of action under the UCL); *Thompson v. Home Depot, Inc.*, No. 07cv1058 IEG, 2007 WL 2746603, at *3 (S.D. Cal. Sept. 18, 2007) (finding that a plaintiff's "personal information" does not constitute property under the UCL). For these reasons, Google's motion to dismiss is granted.

---

[16]Count VI, against Google.

I. The California Consumers Legal Remedies Act[17]

The California Consumer Legal Remedies Act ("CLRA") prohibits "unfair methods of competition and unfair or deceptive acts or practices" in connection with the sale or lease of goods and services. Cal. Civ. Code § 1770. An action may be brought under the CLRA pursuant to § 1780(a), which provides that "[any] consumer who suffers any damage as a result of the use or employment by any person of a method, act, or practice declared to be unlawful by Section 1770 may bring an action against such person." *Id.* § 1780(a). "Services" within the context of the CLRA are defined as "work, labor, and services other than a commercial or business use, including services furnished in connection with the sale or repair of goods." *Id.* § 1761(b). "Goods" are defined as "tangible chattels." *Id.* § 1761(a). The CLRA does not apply to the sale or license of software, because software is neither a "good" nor a "service" covered by the CLRA. *See Ferrington v. McAfee*, No. 10–CV–01455, 2010 WL 3910169, at *19 (N.D.Cal. Oct. 5, 2010) (the CLRA is not applicable to a license for the use of software).

Plaintiffs' argument that Google's advertising is a "service" and not software is unavailing, as plaintiffs' use of software browsers and the subsequent software activity is the conduct alleged to be "unfair." The California case law is clear that software and software activity are not covered by the CLRA. *See, e.g., In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, No. 11-2258, 2012 WL 4849054, at *20-21 (S.D. Cal. Oct. 11, 2012) (the CLRA does not impose liability on defendants for a shut down of an online video gaming network, even if the network was meant to be used with a

[17]Count IX, against Google.

device); *Wofford v. Apple Inc.*, No. 11-34, 2011 WL 5445054, at *2 (S.D. Cal. Nov. 9, 2011) (the CLRA does not afford plaintiffs a remedy for damages arising out of the downloading of a free software upgrade). Further, plaintiffs have not pled facts showing a transaction. Plaintiffs did not pay for the advertisements and the contention that their personal information constitutes a form of "payment" to Google "is unsupported by law." *Facebook*, 791 F. Supp. 2d at 717; *see also Yunker v. Pandora Media, Inc.*, No. 11-3113, 2013 WL 1282980, at *12 (N.D. Cal. Mar. 26, 2013) (dismissing CLRA claim where plaintiff alleged "he purchased the defendant's services with his PII" and not with money). Software and software activity is not covered by the CLRA, making plaintiffs' claim legally deficient. Therefore, Google's motion to dismiss this count is granted.

V. CONCLUSION

For the above reasons, defendants' motions to dismiss are granted. Google's request for judicial notice (D.I. 58) is denied as moot as the court did not rely on the referenced documents.