UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN RE NICKELODEON CONSUMER PRIVACY LITIGATION	:	Civil Action No. 12-7829 (SRC)(CLW)
	:	Honorable Stanley R. Chesler
	:	Motion Return Date:
	:	April 14, 2014
This Document Relates to: **All Actions**	:	(Oral Argument Requested)
	:	*Document Electronically Filed*

GOOGLE INC.'S BRIEF IN SUPPORT OF ITS MOTION TO DISMISS THE MASTER CONSOLIDATED CLASS ACTION COMPLAINT UNDER FED. R. CIV. P. 12(B)(1) AND 12(B)(6)

Jeffrey J. Greenbaum
SILLS CUMMIS & GROSS P.C.
One Riverfront Plaza
Newark, New Jersey 07102-5400
Telephone: (973) 643-7000
jgreenbaum@sillscummis.com

Colleen Bal
(admitted *pro hac vice*)
Michael H. Rubin
(admitted *pro hac vice*)
WILSON SONSINI GOODRICH & ROSATI, P.C.
One Market Plaza
Spear Tower, Suite 3300
San Francisco, CA 94105-1126
Telephone: (415) 947-2000
cbal@wsgr.com
mrubin@wsgr.com

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

RULES

MISCELLANEOUS

STATEMENT OF THE PROCEEDINGS

In addition to its renowned search and email services, Google also provides advertising services to websites, like the Viacom Nickelodeon websites at issue in this multi-district litigation ("MDL"). While website operators typically generate much of the content displayed to visitors of their sites, many employ advertising services like those that Google offers to deliver ads to their visitors. Viacom is one such website operator.

Plaintiffs' claims against Google challenge its use of the Internet "cookies" that help Google to provide advertising services to Viacom. Cookies are small text files transmitted between a server and a user's Internet browser to promote convenience and customization on the Internet. Cookies are standard fare on the Internet, and for almost 15 years, have been used by innumerable companies to provide beneficial services to consumers. Google uses the "DoubleClick ID" cookie, introduced over a decade ago, in an effort to deliver more relevant ads to users of Viacom's website. Google could never have placed these cookies if it had not been invited by Viacom to do so.

Plaintiffs contend that Google's use of the DoubleClick cookie violates their privacy by collecting Plaintiffs' information. But Plaintiffs' own allegations betray their claim that Google uses the DoubleClick cookie to collect their information. The allegations show that (1) Plaintiffs, through their browsers, voluntarily send

the information directly to Google, and (2) they do so *whether or not cookies are present on their browsers*, in the ordinary operation of the Internet. Master Consolidated Class Action Complaint, Dkt. 42, ("Compl.") ¶¶ 24-31, 39-44, 78, 80, 139, 140. As a matter of law, Plaintiffs have alleged no facts showing Google receipt of this information causes them any harm, and they therefore fail to establish Article III standing. But even if Plaintiffs could overcome that hurdle, their own allegations highlight the fundamental disconnect in their case: there is no causal link between the conduct at issue (Google's alleged use of cookies) and the harm Plaintiffs claim (Google's alleged receipt of information). Because Google's conduct did not cause Plaintiffs any harm, they lack Article III standing and their claims should be dismissed for lack of subject matter jurisdiction.

To the extent Plaintiffs seek to rely on a theory of statutory standing, they fare no better because they have failed to state any plausible claim for relief under the statutes they assert. Courts have time and again rejected the claims asserted by Plaintiffs as a matter of law, including in two prior MDL's specifically addressing use of Google's Doubleclick ID cookie. *See, e.g.*, *In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 2013 U.S. Dist. LEXIS 145727 (D. Del. Oct. 9, 2013) ("*Cookie Litig.*") (currently on appeal)(granting motion to dismiss federal and state privacy claims against use and operation of Doubleclick cookie); *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497 (S.D.N.Y. 2001)(same); *Low*

v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1022-32 (N.D. Cal. 2012) (dismissing SCA and state-law claims challenging LinkedIn's use of cookies); *In re Facebook Privacy Litig*., 2011 U.S. Dist. LEXIS 147345, at *4-20 (N.D. Cal. Nov. 22, 2011) (dismissing Wiretap Act, Stored Communications Act, and state-law claims); *LaCourt v. Specific Media, Inc.*, 2011 U.S. Dist. LEXIS 50543, at *7-21 (C.D. Cal. Apr. 28, 2011) (dismissing federal and state claims).

Google respectfully requests that the action be dismissed in its entirety for lack of Article III standing and for failure to state a claim.

SUMMARY OF THE ARGUMENT

A. Plaintiffs Lack Article III Standing

Google's alleged placement of cookies on Plaintiffs' browsers did not cause them any cognizable injury. Plaintiffs' browsers voluntarily send information to Google in the ordinary operation of the Internet and do so whether or not a cookie is present on their browsers. If a cookie is present on a user's browser, it changes only one thing: the browser sends the *cookie value* to Google along with the same information it would otherwise send. The cookie value is an alphanumeric number automatically set by Google that contains no personal information about the user. It merely allows Google to associate prior information sent to it by the same browser, thereby enabling Google to display more relevant ads to that browser.

While Plaintiffs' Complaint is particularly muddy on this point, the only "injury" they claim is that Google profited from this practice. Compl. ¶¶ 49-59.

But as a matter of law, alleging a benefit to the defendant as opposed to a cognizable harm to themselves is insufficient to establish standing. Because Plaintiffs have not alleged facts establishing that they were harmed through Google's use of the DoubleClick cookie to serve them more relevant ads, the case should be dismissed for lack of standing.

B. Each of Plaintiffs' Claims Fails As A Matter Of Law Because Plaintiffs Do Not Allege Basic Elements Of Their Claims

Plaintiffs do not allege any viable claim for relief:

- The Wiretap Act (Count II) prohibits intentional interception of the contents of communications by persons who are not parties to the communication. *See* 18 U.S.C. § 2511(2)(d). Plaintiffs claim that Google used the DoubleClick cookie to intercept their communications, but are deliberately vague about which communications were intercepted. That is no accident. The only communications Google obtains by having a cookie on a user's browser are communications between the browser and the computers Google uses to serve advertisements. *See* Compl., ¶¶ 24-31, 39-44, 78, 80, 139-140. Google is a party to those communications and therefore cannot be charged with improperly intercepting them under the Wiretap Act or related state law (Counts II and IV). Those claims fail for the additional reason that only the "contents" of a communication, *i.e.*, "information concerning the substance, purport or meaning of th[e] communication" is protected. 18 U.S.C. § 2510(8); Cal. Penal Code § 631.

Google did not receive the contents of any communication due to the presence of DoubleClick cookies on a user's browser; it received only the cookie value it assigned to that browser.

- The Stored Communications Act ("SCA") (Count III) prohibits intentionally accessing without authorization "a facility through which an electronic communication service is provided" to obtain electronic communications "in electronic storage." 18 U.S.C. § 2701(a). It is intended to protect electronic communications stored by *third party communications services*. This claim fails because (i) Plaintiffs allege that the communications at issue were obtained while *in transit*, not in "*storage*"; (ii) their own computers do not constitute "facilities" under the SCA; and (iii) Plaintiffs voluntarily sent their communications to Google; Google did not access them "without authorization."

- The Video Privacy Protection Act ("VPPA") (Count I) prohibits knowing disclosures by a "video tape service provider" ("VTSP") of "information that identifies a person as having requested or obtained specific video materials" ("PII") from a VTSP. Plaintiffs' VPPA disclosure claim fails because (i) Plaintiffs do not allege that Google is a VTSP; and (ii) Plaintiffs do not allege facts showing that Google disclosed Plaintiffs' PII to anyone. The VPPA also prohibits VTSP's from retaining PII for more than a year longer than necessary. Plaintiffs' VPPA retention claim fails because (i) Google is not a VTSP; (ii) it did not receive

Plaintiffs' PII; (iii) there is no private cause of action for a retention claim; and (iv) Plaintiffs allege no facts showing Google retained their PII longer than necessary.

- The New Jersey Computer Related Offenses Act ("CROA") Claim (Count V) fails because (i) Plaintiffs were not "damaged in business or property"; (ii) Google did not purposefully or knowingly harm Plaintiffs; and (iii) Plaintiffs do not allege facts to satisfy the elements of any subsection of the CROA.

- The "intrusion" claim (Count VI) fails because (i) assuming counterfactually that placing cookies on Plaintiffs' browsers was unlawful (contrary to all precedent), Plaintiffs allege no facts showing that Google knew and intended such illegality; (ii) Google obtained no private information; and (iii) the alleged intrusion was not highly offensive because cookies are standard, well-known, and fundamental to the provision of countless Internet services.

- The unjust enrichment claim (Count VII) fails because (i) Plaintiffs do not invoke the law of any jurisdiction; and (ii) unjust enrichment is not a cause of action under California law and fails to state a claim under New Jersey law.

STATEMENT OF FACTS

A. The Ubiquitous Use Of Cookies On The Internet

Internet "cookies" are small text files that are transmitted between a website and an Internet browser. Compl. ¶ 33; *Cookie Litig.*, 2013 U.S. Dist. LEXIS 145727, at *4. "Cookies are widely used on the Internet by reputable websites to promote convenience and customization." *In re Pharmatrak, Inc.*, 329 F.3d 9, 14

(1st Cir. 2003)*; see* Compl. ¶¶ 34, 35, 37; *Netscape Commc'ns Corp. v. ValueClick, Inc.*, 684 F. Supp. 2d 678, 682 (E.D. Va. 2009) ("[T]oday the 'cookies' technology is ubiquitous, and plays a large role in Internet users' Web browsing."); *DoubleClick*, 154 F. Supp. 2d at 504 (service created to serve tailored ads using cookies over twelve years ago). Cookies allow websites to retain the contents of users' online shopping carts, keep users logged into sites between visits, and store users' preferences. *Pharmatrack*, 329 F.3d at 14. Cookies are useful for Internet advertising because they allow for the display of more relevant ads to browsers. Compl. ¶¶ 37, 38, 39, 47, 48, 69, 71.

B. Plaintiffs' Browsers Send Information To Google Through GET Commands, Whether Or Not A Cookie Is Present

Plaintiffs' Complaint describes how their browsers send information to Google, *even in the absence of cookies*, so that Google can provide advertising services to websites by displaying ads to Plaintiffs when they visit those websites. *See generally id.* ¶¶ 24-31, 39-44, 78, 80, 139, 140.[1]

Each website on the Internet is hosted by a computer server. Compl. ¶ 25. To access a website, people use browsers to communicate with these servers. *Id.* ¶¶ 24-25. When a web address, known as a Uniform Resource Locator ("URL")

[1] Google accepts the allegations as true only for purposes of this motion to dismiss, and would dispute many of them if the case were to continue.

such as "www.cnn.com," is entered into a browser's address bar, the browser submits a "GET" command to the website seeking all content displayed on the site. *Id.* ¶¶ 26, 27, 46. This GET command includes certain information generated by the browser that enables the website to display the correct content. *See id.* ¶¶ 27, 31; *DoubleClick*, 154 F. Supp. 2d at 503 ("This communication may contain data submitted as part of the request, such as a query string or field information.").

If the website wishes to display an ad, the website will instruct *the browser* to send a separate GET command to an ad service. Compl. ¶¶ 30, 31, 40, 46. Where the ad service is Google, the browser voluntarily sends a GET command to Google. The GET command contains information generated by the browser necessary to ensure that the correct ad is displayed. *See DoubleClick*, 154 F. Supp. 2d at 503. Plaintiffs allege that the GET command transmits information, including the URL of the page that the user is visiting and other "personal information." *See* Compl. ¶ 42 ("In many cases, the third party *receives the re-directed "GET" request and a copy of the user's request to the first-party website* before the content of the initial request from the first-party webpage appears on the user's screen.") (emphasis added); *id.* ¶ 139 (alleging "[t]he specific Uniform Resource Locators the Plaintiffs typed into *and sent through their web browsers* are 'contents'. . .") (emphasis added); *id.* ¶ 140 (asserting legal conclusion that URL "is content because . . . . it identifies the exact title of the video shown on the

communication requested and received by the Internet user from Viacom"); *see also id.* ¶¶ 24-31, 39-41, 43-44, 78, 177. This information, including the URL, is transmitted to Google by the user's browser, *whether or not a cookie is present on the user's browser*. *See* Compl. ¶¶ 24-31, 39-44, 78, 80, 139, 140; *Cookie Litig.*, 2013 U.S. Dist. LEXIS 145727, at *15 ("plaintiffs' browsers voluntarily sent to Google the information inputted by plaintiffs [as part of the GET command], regardless of whether plaintiffs' browsers had any Google cookies set"); *id.* at *16 ("[P]laintiffs' browsers would send a URL [to Google as part of the GET command] regardless of whether a third party cookie was set.").

Google responds to this GET command by selecting and sending an ad for display in the browser. Compl. ¶¶ 31, 44. An ad will be displayed to the user whether or not a cookie is present on the user's browser. *Id.* ¶¶ 28-31, 39-44. If a DoubleClick cookie *is not* already present and the browser is configured to accept cookies, a cookie may be placed on the browser. *See id.* ¶¶ 45, 46, 73, 74.

C. DoubleClick Cookies Allow Google To Send More Relevant Ads

If a DoubleClick cookie *is present* on a browser that visits a webpage that displays a Google ad, the cookie value – the alphanumeric number assigned to Plaintiffs' browser by Google – is sent by the browser to Google as part of the GET command. *See id.* ¶¶ 45, 47, 48; *Pharmatrak*, 329 F.3d at 14 ("A cookie is a piece of information sent by a web server to a web browser that the browser

software is expected to save and to send back whenever the browser makes additional requests of the server."). Plaintiffs do not allege that any additional or different information is sent from their browsers to Google in the GET command when a cookie is present, other than the cookie value itself.

The string of text that makes up the DoubleClick cookie value does not include the contents of any communication. It is merely an "alphanumeric identifier" unrelated to the communication it accompanies. *See* Compl. ¶¶ 47, 98; *see also DoubleClick*, 154 F. Supp. 2d at 513. The cookie value allows Google to present more relevant ads to the browser at the next page the browser visits that employs Google's ad services. *See* Compl. ¶¶ 35, 47. 48, 69, 77, 82, 83, 94; *DoubleClick*, 154 F. Supp. 2d at 505; *see also Cookie Litig.*, 2013 U.S. Dist. LEXIS 145727, at *4-5; *Pharmatrak*, 329 F.3d at 14. Google can recognize the browser from the cookie value, and tailor ads based on prior experiences of the browser's user(s). Compl. ¶¶ 37-39, 47, 48, 69, 71, 84; *DoubleClick*, 154 F. Supp. 2d at 503.

D. User Information Collected by Viacom Is Unknown to Google

Plaintiffs contend that Viacom collects birth date and gender information from visitors to its Nickelodeon websites who register and establish profiles with them. Compl. ¶85-86. Plaintiffs allege that Viacom assigns internal codes (called the "rugrat coding") to its users based on their age and gender. *Id.*, ¶¶ 88-89. But

Plaintiffs admit that to the extent this information is provided to Google, it is in *coded form*. *Id.*, ¶¶ 93, 98, 99. They do not allege that Google is aware of the information, much less that Google understands Viacom's internal "rugrat" codes.

E. The Complaint and The Named Plaintiffs

This multi-district litigation comprises six federal civil actions filed against Viacom and Google, all of which were transferred to this Court. Dkt. 31. The named plaintiffs are all under the age of thirteen and allege that they were registered users of at least one of the following Viacom websites: Nick.com, NickJr.com, and NeoPets.com. *Id.* They claim that when they visited these sites, Google placed cookies on their browsers without their consent. Plaintiffs assert various federal and state claims, seeking to represent a putative class.[2]

ARGUMENT

I. THIS ACTION SHOULD BE DISMISSED UNDER RULE 12(B)(1) BECAUSE PLAINTIFFS LACK ARTICLE III STANDING

The action should be dismissed under Rule 12(b)(1) because Plaintiffs have not suffered an Article III injury. A suit brought by a plaintiff without Article III

---

[2] The class is defined as "[a]ll children under the age of 13 in the United States who visited the websites Nick.com, NickJr.com, and/or NeoPets.com, and had Internet cookies that tracked their Internet communications placed on their computing devices by Viacom and Google." A subclass is defined as "[a]ll children under the age of 13 in the United States who were registered users of Nick.com, NickJr.com, and/or NeoPets.com, who engaged with one or more video materials on such site(s), and who had their video viewing histories knowingly disclosed by Viacom to Google." Compl. ¶ 103.

standing does not meet the Constitution's "case or controversy" requirement. *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 101, 109-110 (1998). "[T]o satisfy Article III's standing requirements, a plaintiff must show (1) it has suffered an 'injury in fact' that is (a) concrete and particularized and (b) actual or imminent, not conjectural or hypothetical; (2) the injury is fairly traceable to the challenged action of the defendant; and (3) it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision." *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 180-181 (2000). The plaintiff "bears the burden of establishing that he has Article III standing for each type of relief sought." *ZF Meritor, LLC v. Eaton Corp.*, 696 F.3d 254, 301 (3d Cir. 2012).

In putative class actions alleging supposed privacy violations, court after court has found there to be no Article III injury where a plaintiff makes nothing more than the type of general allegations Plaintiffs make here. Compl. ¶¶ 49-59.[3]

---

[3] A host of these cases involve allegations of supposedly nefarious cookie use. *See, e.g.*, *In re Google Inc. Privacy Policy Litig.*, 2013 U.S. Dist. LEXIS 171124, at *15 (N.D. Cal. Dec. 3, 2013) ("*Google Privacy Litig. II*") ("injury-in-fact in this context requires more than an allegation that a defendant profited from a plaintiff's personal identification information"); *Cookie Litig.*, 2013 U.S. Dist. LEXIS 145727, at *8, 10 (allegations that personal information "has value to third-party companies" does not "equate . . . to injury in fact"); *In re Google Inc. Privacy Policy Litig.*, 2012 U.S. Dist. LEXIS 183041, at *17 (N.D. Cal. Dec. 28, 2012) ("*Google Privacy Policy Litig. I*") (the law does not confer "standing on a party that has brought statutory or common law claims based on nothing more than the unauthorized disclosure of personal information"); *Low v. LinkedIn Corp.*, No.: (continued...)

For example in *LaCourt*, plaintiffs accused an online advertising network of using cookies to track their Internet use without consent. 2011 U.S. Dist. LEXIS 50543, at *2-4. The court held plaintiffs lacked standing because they had not alleged (1) that any named plaintiff was actually harmed, or (2) any "particularized" injury. Plaintiffs' resort to abstract concepts like "opportunity costs" were insufficient. *Id.* at *7-15. Similarly, in *Del Vecchio I*, plaintiffs accused Amazon.com of placing cookies on their browsers "against their wishes." 2011 U.S. Dist. LEXIS 138314, at *3. Plaintiffs asserted that use of cookies to obtain their information caused them "'economic harms,' including "loss of the economic value of the information." *Id.* at *4. The court dismissed the case for failure to plead facts demonstrating "any plausible harm." *Id.* at *22.

Plaintiffs' counsel are no strangers to this extensive body of law. They briefed (and lost) this precise issue in *Cookie Litig*. There, as here, plaintiffs alleged they suffered an injury by Google's placement of DoubleClick cookies on

---

(...continued from previous page)
11-CV-01468, 2011 U.S. Dist. LEXIS 130840, at *10-15 (N.D. Cal. Nov. 11, 2011) (dismissing for lack of standing claims that relied on general allegations that consumer information is valuable); *LaCourt*, 2011 U.S. Dist. LEXIS 50543, at *12 (same); *Del Vecchio v. Amazon.com Inc.*, 2011 U.S. Dist. LEXIS 138314, at *10 (W.D. Wash. Dec. 1, 2011) ("*Del Vecchio I*") ("While it may be theoretically possible that Plaintiffs' information could lose value as a result of its collection and use by Defendant, Plaintiffs do not plead any facts from which the Court can reasonably infer that such devaluation occurred in this case."); *In re JetBlue Airways Corp. Privacy Litig.*, 379 F. Supp. 2d 299, 327 (E.D.N.Y. 2005).

their browsers, asserting that the cookies enabled Google to collect their "personal information." 2013 U.S. Dist. LEXIS 145727, at *7-12. Plaintiffs "cite[d] to many articles to support their allegations that personally identifiable information ('PII') has monetary value and is a commodity that companies trade and sell." *Id.* at *7-8. The court held plaintiffs lacked standing because they had "not sufficiently alleged that the ability to monetize their PII has been diminished or lost by virtue of Google's previous collection of it." *Id.* at *10-11.

That reasoning applies with equal force here. Plaintiffs cite articles to try to show that online personal information has monetary value. Compl. ¶¶ 49-59. But such allegations have repeatedly been found insufficient as a matter of law. *E.g.*, *Cookies Litig.*, 2013 U.S. Dist. LEXIS 145727, at *8; *Low*, 2011 U.S. Dist. LEXIS 130840, at *10-15; *LaCourt*, 2011 U.S. Dist. LEXIS 50543, at *12; *Del Vecchio I*, 2011 U.S. Dist. LEXIS 138314, at *10. Plaintiffs do not allege facts to show their ability to monetize their personal information was diminished. They do not allege that they attempted to sell their information or were unable to do so because of Google. Thus, they do not establish an actual concrete injury.

Plaintiffs not only fail to establish actual injury, they also fail to state a plausible violation of any statute that might confer statutory standing. While it is by no means clear that plaintiffs who have suffered no injury-in-fact can bring a claim under the Wiretap Act, SCA or VPPA, it is clear that they must, at a

minimum, state a claim under those statutes to be able to invoke a theory of statutory standing. *See, e.g.*, 18 U.S.C. § 2520(a) (Wiretap Act standing requires facts showing plaintiffs' communications were "intercepted, disclosed, or intentionally used in violation of [the Wiretap Act]"); 18 U.S.C. § 2707(a) (SCA standing requires facts showing plaintiffs were "aggrieved by any violation of [the SCA]"); 18 U.S.C. § 2710(c)(1) (VPPA standing requires facts showing plaintiffs were "aggrieved by any act of a person in violation of this section"); *e.g.*, *Sterk v. Best Buy Stores, L.P.*, 2012 U.S. Dist. LEXIS 150872, at *16-17 (N.D. Ill. Oct. 17, 2012) ("plaintiff must plead [both] an injury [and] a statutory violation to meet the standing requirement of Article III [for an SCA claim and a VPPA claim]"). As shown below in connection with our Rule 12(b)(6) argument, Plaintiffs have not stated a claim under any of the federal statutes they assert. Because they have not alleged injury-in-fact or established statutory standing, the action should be dismissed for lack of subject matter jurisdiction.

II. THIS ACTION SHOULD BE DISMISSED UNDER RULE 12(B)(6) FOR FAILURE AND INABILITY TO STATE A CLAIM

A. Legal Standard

Under Rule 12(b)(6), a complaint must be dismissed when it "fail[s] to state a claim upon which relief can be granted." Fed. R. Civ. P. 12(b)(6). "[O]nly a complaint that states a plausible claim for relief survives a motion to dismiss." *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009); *Connelly v. Steel Valley Sch. Dist.*,

706 F.3d 209, 212 (3d Cir. 2013). "Threadbare recitals of the elements . . . do not suffice." *Iqbal*, 556 U.S. at 678. The court must "disregard 'naked assertions devoid of further factual enhancement.'" *Santiago v. Warminster Twp.*, 629 F.3d 121, 131 (3d Cir. 2010). Thus, while the Court accepts as true all material allegations, it need not accept as true conclusory allegations, unwarranted inferences, or legal conclusions cast in the form of factual allegations. *Iqbal*, 556 U.S. at 678-79; *Santiago*, 629 F.3d at 131-133. Because Plaintiffs have not stated a viable claim against Google, the action should also be dismissed for failure to state a claim.

B. The Wiretap Claim (Count II) Should Be Dismissed

The Wiretap Act (a) protects only against intentional interception of a communication by persons who are *not* parties to that communication, and (b) only applies where the *contents* of the communication were improperly intercepted. *Bartnicki v. Vopper*, 532 U.S. 514, 523 (2001); *United States v. Reed*, 575 F.3d 900, 916 (9th Cir. 2009). Here, the only communications Plaintiffs identify as potentially intercepted by Google were GET commands sent from Plaintiffs' browsers to Google. *See* Compl. ¶¶ 30, 31, 40, 46.[4] Plaintiff therefore have no

[4] Plaintiffs also allege that Google intercepted "Plaintiffs' communications with the Viacom children's websites." Compl., ¶ 154. But Plaintiffs do not identify any such communications or otherwise provide factual support for this (continued...)

viable Wiretap Act claim because (1) Google is a party to the communications and thus cannot be held liable for unlawful interception, and (2) the only information Google received from Plaintiffs due to the placement of cookies were the cookie values themselves, which are not protected "contents." 18 U.S.C. § 2510(8).

1. Google Was A Party To The Communications

It is not unlawful for a "party to the communication" to receive the communication. 18 U.S.C. § 2511(2)(d). Google was a party to any plausible "communication" here because the exchange of information was in the form of GET commands sent from Plaintiffs' browsers to Google. As Plaintiffs allege:

> Upon receiving a GET command from a child's web browser, the website host server contemporaneously instructs the child's web browser *to send other GET commands to other servers responsible for filling in the blank parts of the web page*.

(...continued from previous page)
conclusory allegation (and to the contrary, only identify communications sent directly from Plaintiff to Google, *see, e.g.*, *id*. ¶¶ 30, 31, 40, 46). The allegation is therefore properly disregarded. *Iqbal*, 556 U.S. at 678. But even if Google were not a party to the communications, and instead had intercepted communications between Plaintiffs and the Viacom websites, Plaintiffs would still not state a Wiretap Act claim. The websites that Plaintiffs allegedly visit were also parties to the communications with Plaintiffs' browsers, and those websites have authorized Google's access to the communications. Compl., ¶¶ 38-42, 74, 97, 128. This prior consent defeats an interception claim. *See* 18 U.S.C. 2511(2)(d); *DoubleClick*, 154 F. Supp. 2d at 510, 514 ("DoubleClick affiliated Web sites are 'parties to the communication[s]' from [browsers] and have given sufficient consent to DoubleClick to intercept them.").

Compl. ¶ 30 (emphasis added); *see also id*. ¶¶ 24-29, 31, 39-44, 78, 80, 139-140. Plaintiffs' browsers send the GET commands to Google in the ordinary operation of the Internet because the GET commands contain information Google needs to display ads. *See* Compl. ¶¶ 25-27, 30-31, 40-44; *DoubleClick*, 154 F. Supp. 2d at 503. They send the GET commands whether or not DoubleClick cookies are present. *See* Compl. ¶¶ 24-31, 39-44, 78, 80, 139, 140; *Cookie Litig.*, 2013 U.S. Dist. LEXIS 145727, at *15-16. And according to Plaintiffs, it is the GET commands that contain the "personal information" at issue, including the URLs of websites. *See* Compl. ¶¶ 78, 80, 139-40, 177. Because Google cannot "intercept" communications Plaintiffs send directly to it, their claim fails. *See, e.g.*, *Goode v. Goode*, 2000 U.S. Dist. LEXIS 3124, at *8 (D. Del. Mar. 14, 2000).

To try to avoid dismissal of their Wiretap Act claim on the ground that they voluntarily send the information at issue directly to Google, Plaintiffs seek to invoke an exception under the Act, which permits parties to communications to be held liable if they intercept the communications "for the purpose of committing a[] criminal or tortious act." Compl. ¶¶ 153-54; 18 U.S.C. § 2511(2)(d). But Plaintiffs misunderstand this narrow exception. It applies only "if [the interception was] made 'with an unlawful *motive*,' such as 'blackmailing the other party, threatening him, or publicly embarrassing him.'" *Caro v. Weintraub,* 618 F.3d 94, 99 (2d Cir. 2010) (emphasis added). Plaintiffs would therefore need to allege that

Google had "as [its] *objective* a tortious or criminal result," *id.* at 100 (emphasis added),[5] and that the tortious or criminal act was "*independent* of the intentional act" of interception. *Id.* (emphasis added); *Berk v. J.P. Morgan Chase Bank, N.A.*, 2011 U.S. Dist. LEXIS 143510 (E.D. Pa. Dec. 13, 2011).

Plaintiffs' own allegations demonstrate the inapplicability of this exception, as Plaintiffs concede that Google's purpose was to provide a valued service to commercial websites, and not to perpetuate a tort or crime. *See, e.g.*, Compl. ¶ 2 ("[U]nique and specific electronic identifying information and content about each of these children was accessed, stored, and utilized *for commercial purposes*.") (emphasis added); *DoubleClick*, 154 F. Supp. 2d at 518 (rejecting application of criminal purpose exception where use of DoubleClick cookie was to "execut[e] a highly-publicized market-financed business model in pursuit of commercial gain"). While Plaintiffs also assert that "the [D]efendants' actions were done for criminal purposes in violation of numerous federal and state statutes, including, but not limited to 18 U.S.C. § 1030(a)(2)(C) of the Computer Fraud and Abuse Act ["CFAA"]" (Compl. ¶ 154) and that "Defendants' actions were done for the

---

[5] *See also Sussman v. American Broad. Cos.*, 186 F.3d 1200, 1202-03 (9th Cir. 1999) ("Where the purpose is not illegal or tortious, but the means are, the victims must seek redress elsewhere"); *DoubleClick*, 154 F. Supp. 2d at 516 ("[A] plaintiff cannot establish that a defendant acted with a 'criminal or tortious' purpose simply by proving that the defendant committed any tort or crime.").

tortious purpose of intruding upon the Plaintiffs' seclusion as set forth in this Complaint" (*Id.* ¶ 153), those allegations are mere "formulaic recitation[s]" without support. They are properly ignored.[6] *Iqbal*, 556 U.S. at 678.

2. Google Did Not Intercept Any "Contents"

Plaintiffs' claim must be dismissed for the additional reason that they do not allege that Google intercepted the "contents" of their communications. 18 U.S.C. § 2510(4) (defining "intercept"); § 2511(1); *Walsh v. Krantz*, 386 F. App'x 334, 338-339 (3d Cir. 2010); *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113-114 (3d Cir. 2004). "Contents" is defined to cover only "information concerning the substance, purport, or meaning of" the communication. 18 U.S.C. § 2510(8); *see Cookie Litig.*, 2013 U.S. Dist. LEXIS 145727, at *14-15; *Reed*, 575 F.3d at 916; *Gilday v. Dubois*, 124 F.3d 277, 296 n.27 (1st Cir. 1997). The Act thus protects only the substance of communications *intentionally communicated* from one person to another, "such as the words spoken in a phone call." *In re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1061 (N.D. Cal. 2012) ("*iPhone II*"). It does not protect transactional information, such as a party's identity, when or

[6] Even if considered, the allegations are nonsensical. The exception applies where the interception is undertaken to enable further tortious or criminal conduct, such as blackmail. Plaintiffs contend that placing cookies itself constitutes a CFAA-like violation, not that placing cookies somehow enables Google to violate the CFAA. *See infra* at pp. 33-37.

where the communications took place, or the length of the communications. *See, e.g., Sams v. Yahoo!, Inc.*, No. 10-5897, 2011 WL 1884633, at *6-7 (N.D. Cal. May 18, 2011) (Act does not cover records identifying person using Yahoo ID and email address, IP addresses, and login times); *Jessup-Morgan v. Am. Online, Inc.*, 20 F. Supp. 2d 1105, 1109 (E.D. Mich. 1998) (identity of user not covered); *Reed*, 575 F.3d at 916 (time of origination, duration, source, and destination of telephone call not covered); *Gilday*, 124 F.3d at 296 n.27 (Act does not cover "the PIN of [a] caller, the number called, and the date, time[,] and length of the call").

In the Internet context, "personally identifiable information that is automatically generated by the communication" is not "'contents' for the purpose of the Wiretap Act." *Cookie Litig.*, 2013 U.S. Dist. LEXIS 145727, at *15-16; *iPhone II*, 844 F. Supp. 2d at 1061-62 (data conveying geolocation of iPhone users not covered by the Wiretap Act); *In re § 2703(d) Order*, 787 F. Supp. 2d 430, 435-36 (E.D. Va. 2011) (Act does not cover IP numbers, Twitter subscriber, user, and screen names, e-mail addresses, telephone and instrument numbers, subscriber numbers and identities, and temporarily assigned network addresses).

Plaintiffs have not alleged that contents of communications were intercepted as a result of Google's placement of the Doubleclick cookie, the only "interceptions" even potentially at issue. *See*, *e.g.*, Compl. ¶¶ 137-38 ("Google intentionally intercepted the contents of electronic communications . . . through

Google's use of devices that tracked and recorded the Plaintiffs' web communications," namely "Google's DoubleClick.net cookies"); *id.* ¶ 155 ("Google used the cookies" "to intercept[] the Plaintiffs' communications with the Viacom children's websites"). Plaintiffs' browsers send GET commands even in the absence of any cookies; Plaintiffs do not and cannot allege that Google "intercepted" any new or different information due to the presence of the DoubleClick cookie. *See id*. ¶¶ 24-31, 39-44, 78, 80, 139-40; *Cookie Litig.*, 2013 U.S. Dist. LEXIS 145727, at *15 ("plaintiffs' browsers voluntarily sent to Google the information inputted by plaintiffs, regardless of whether plaintiffs' browsers had any Google cookies set"); *id.* at *16 ("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.").

Thus, the *only* information that would not have been communicated to Google but for the placement of the cookie is the cookie's value. *See* Compl. ¶¶ 45, 47-48. But cookie value is merely an "alphanumeric identifier" unrelated to the communication it accompanies. *See id.* ¶¶ 47, 98; *DoubleClick*, 154 Supp. 2d at 513 (cookie id number is "meaningless to anyone" other than Google). Because it conveys no information concerning the substance, purport, or meaning of Plaintiffs' communications, the cookie value is not protected "contents."

3. Because There Was No Unlawful Interception, Plaintiffs Cannot State Use And Disclosure Claims

Plaintiffs make vague and conclusory allegations that Google "disclosed" and "used" unlawfully intercepted communications. *See* Compl. ¶ 159. Those conclusory allegations, devoid of specific facts, are properly disregarded. In any event, because Plaintiffs cannot show any unlawful interception, they cannot show an unlawful disclosure or use. 18 U.S.C. § 2511(1)(c)-(d) (creating liability only for use and disclosure of information "obtained in violation of this subsection").[7]

C. The California Invasion of Privacy Act Claim Should Be Dismissed (Count IV)

Plaintiffs cannot state a California Invasion of Privacy Act, Penal Code § 631 ("CIPA") claim for the same reasons they cannot state a Wiretap Act claim. They cannot show that Google "in any unauthorized manner," intercepted, used, or disclosed the "contents or meaning" of a "communication" that is "in transit."[8] *Id.* § 631(a); Compl. ¶ 176. In particular:

---

[7] *See also In re High Fructose Corn Syrup Antitrust Litig.*, 216 F.3d 621, 625 (7th Cir. 2000); *Meredith v. Gavin*, 446 F.2d 794, 799 (8th Cir. 1971); *Buckingham v. Gailor*, No. 00-1568, 2001 WL 34036325, at *6 (D. Md. Mar. 27, 2001), *aff'd*, 20 F. App'x 243 (4th Cir. 2001); *Betancourt v. Nippy, Inc.*, 137 F. Supp. 2d 27, 31-32 (D.P.R. 2001); *Simmons v. Sw. Bell Tel. Co.*, 452 F. Supp. 392, 396-97 (W.D. Okla. 1978), *aff'd*, 611 F.2d 342 (10th Cir. 1979).

[8] Even if Plaintiffs could allege a claim, it would be preempted by the federal Wiretap Act. *In re Google Inc. St. View Elec. Commc'ns Litig.*, 794 F. Supp. 2d 1067, 1084-85 (N.D. Cal. 2011); *LaCourt*, 2011 U.S. Dist. LEXIS 50543, at *7; (continued...)

(1) Google was an authorized party to the communication. *Membrila v. Receivables Performance Mgmt.*, 2010 U.S. Dist. LEXIS 33565, at *4 (S.D. Cal. Apr. 6, 2010) ("Section 631 . . . applies only to eavesdropping by a third party and not to recording by a participant to a conversation."); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 713 (N.D. Cal. 2011); and

(2) Plaintiffs fail to allege the interception of the content of a protected communication. Cal. Pen. Code § 631(a); *Cookie Litig.*, 2013 U.S. Dist. LEXIS 145727, at *19 (substantively identical "allegations d[id] not demonstrate that Google intercepted any 'contents or meaning.'"); *People v. Suite*, 161 Cal. Rptr. 825, 828 (Cal. Ct. App. 1980) (obtaining telephone numbers of callers does not reveal contents of communications).

D. The Stored Communications Act Claim (Count III) Should Be Dismissed

The Stored Communications Act ("SCA") 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) (emphasis added).

(...continued from previous page)
Bunnell v. Motion Picture Ass'n of Am., 567 F. Supp. 2d 1148, 1154-55 (C.D. Cal. 2007).

1. Plaintiffs Cannot Identify A Communication In Electronic Storage

Plaintiffs' SCA claim is irreconcilable with their Wiretap Act claim. Plaintiffs contend that Google improperly accessed electronic communications from their "web browsers" and "computing devices" (Compl. ¶¶170, 173), but the only such communications they identify are the GET requests Plaintiffs' browsers send to Google. *Id.* ¶¶ 24-31, 39-44, 78, 80, 139-140. Plaintiffs go to great lengths to show that these communications were "in transit" and accessed "contemporaneously with the Plaintiffs' communications," *e.g.*, *Id,*¶¶ 30, 145, as required by the Wiretap Act, *see Fraser*, 352 F.3d at 113. Those allegations preclude the SCA claim—which requires communications to be accessed while in "electronic storage." 18 U.S.C. § 2701(a); *see Callaway Golf Co. v. Dunlop Slazenger Grp. Am., Inc.*, 295 F. Supp. 2d 430, 438 (D. Del 2003) (plaintiffs "may plead alternative theories of relief based on the same set of facts," but may not plead inconsistent facts). Because communications cannot simultaneously be "in transit" and in "storage," Plaintiffs' SCA claim fails. *Fraser*, 352 F.3d at 114.

2. Plaintiffs Cannot Identify A Facility Under The SCA

The lack of an SCA-covered "facility" is also fatal to Plaintiffs' claim. *E.g.*, *Cookie Litig.*, 2013 U.S. Dist. LEXIS 145727, at *26-27. Congress enacted the SCA out of concern that the Fourth Amendment might not protect against searches and seizures of electronic communications stored by *third party* communications

services, and therefore sought to fill that gap by protecting against unauthorized access when they were in such hands. *Id*. at *20-21. Thus, the "facilities" the SCA covers are those of "providers of a communication service such as telephone companies, Internet or e-mail service providers, and bulletin board services." *Garcia v. City of Laredo*, 702 F.3d 788, 792 (5th Cir. 2012). While Plaintiffs recite the words of the statute in claiming that their personal computing devices (and by extension web browsers) are SCA "facilities" (Compl. ¶¶ 169, 171), courts have overwhelmingly (and rightly) rejected that nonsensical interpretation. *See Garcia*, 702 F.3d at 792-93; *Morgan v. Preston*, No. 3:13-00403, 2013 U.S. Dist. LEXIS 159641, at 14 & n.3 (M.D. Tenn. Nov. 7, 2013) ("the overwhelming body of law" holds that an individual's personal computer is not a 'facility'"); *Cookie Litig.*, 2013 U.S. Dist. LEXIS 145727, at *24.

Plaintiffs' interpretation would "render other parts of the statute illogical." *iPhone II*, 844 F. Supp. 2d at 1058. If Plaintiffs were right and their personal computers were "facilities," then § 2701(c) would permit Internet and email service providers to "grant access to a user's computer (the 'facility')." *Id*. "'It would certainly seem odd that the provider of a communication service could grant access to one's home computer to third parties, but that would be the result of [plaintiff's] argument.'" *Id.* (citation omitted)); *see also Cookie Litig.*, 2013 U.S.

Dist. LEXIS 145727, at *23 (this interpretation "confounds the distinction between 'users' and 'providers' which, in turn . . . [makes] . . . § 2701(c) nonsensical").

3. Plaintiffs Cannot Show That Google's Access Was Unauthorized

Plaintiffs also cannot show that Google's access to its own cookies was unauthorized. Years ago, the *DoubleClick* court dismissed plaintiffs' SCA claim on this basis, holding that DoubleClick was authorized to access its cookies. 154 F. Supp. 2d at 513-14. What was true then remains so today. Moreover, Plaintiffs authorized access because their browsers voluntarily sent cookie values to Google.

E. The Video Privacy Protection Act Claim (Count I) Should Be Dismissed

Plaintiffs' claim under the Video Privacy Protection Act ("VPPA") must be dismissed. The VPPA was enacted in 1988 after the *City Paper* published a list of videos that Supreme Court nominee Judge Robert Bork had rented from a video store. *See* S. Rep. 599, 2nd Sess., at 5 (Oct. 5, 1988). Congress thus passed the VPPA to govern the circumstances in which a "video tape service provider" (or "VTSP") may disclose "personally identifiable information" to third-parties (18 U.S.C. § 2710(b)) and for how long the VTSP may retain it (18 U.S.C. § 2710(e)).

1. Plaintiffs Fail To Plead A Disclosure Claim

The VPPA prohibits (1) a VTSP (2) from "knowingly disclos[ing] to any person" (3) personally identifiable information ("PII") (4) "concerning any

consumer of such provider," unless an exception applies. 18 U.S.C. § 2710(a)(3), (a)(4), (b)(1), (b)(2). Plaintiffs fail to plead a viable disclosure claim.

i. Google Is Not A VTSP

A VTSP is a "person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials." *Id.* § 2710(a)(4). Plaintiffs cannot allege that Google satisfies this definition, and they do not even try. *See* Compl. ¶ 126 (only attempting to plead facts establishing that Viacom satisfies definition). While Plaintiffs' theory of liability is far from clear, they apparently contend Google satisfies the alternate definition of a VTSP: an "entity to whom a disclosure is made" *by another VTSP*. *See* 18 U.S.C. § 2710(a)(4) (emphasis added); §2710(b)(2)(D) & (E). Plaintiffs claim Google "obtain[ed] Plaintiffs' personally identifiable information in the form of the specific video materials and services requested and obtained . . . *from Viacom*." Compl. ¶ 129 (emphasis added).

Even if Viacom were a VTSP, Google is not an entity to whom a disclosure was made by another VTSP because *Viacom* did not disclose PII to Google, *i.e.,* "information which identifies [Plaintiffs] as having requested or obtained specific video materials from [Viacom]." 18 U.S.C. § 2710(a)(3). If PII were disclosed to Google (which it was not), it would have been disclosed *by Plaintiffs themselves*, not by Viacom. Plaintiffs admit this. They allege that the URLs they *"typed into*

and sent through their web browsers" identify the videos they requested and received from Viacom. Compl. ¶¶ 139-40; *see also id.* ¶¶ 78, 80. As discussed above (*see supra* pp. 7-9, 17-20), Plaintiffs voluntarily transmit the URLs to Google as part of their GET command requesting ad content. *See Cookie Litig.*, 2013 U.S. Dist. LEXIS 145727, at *16. Thus, even if the exact titles of videos viewed by Plaintiffs were disclosed (which they were not), they were disclosed to Google *by Plaintiffs*, not by Viacom. Google is therefore not a VTSP and cannot be held liable under the VPPA.[9] 18 U.S.C. § 2710(b)(1).

ii. Google Did Not Disclose Plaintiffs' PII

Plaintiffs' VPPA claim also fails because they do not allege Google knowingly disclosed PII to any third party. Compl. ¶¶129-130 (alleging that Google "obtain[ed]" PII, but not alleging that Google disclosed it); 18 U.S.C. § 2710(b)(1); *Mollett v. Netflix, Inc.*, No. 5:11-CV-01629, 2012 U.S. Dist. LEXIS 116497, at *11 (N.D. Cal. Aug. 17, 2012). In *Rodriguez v. Sony Computer Entm't*

[9] To the extent *Dirkes v. Borough of Runnemede* can be read to say that "any person" can violate the disclosure provisions of the VPPA, not just a VTSP, it was wrongly decided. 936 F. Supp. 235 (D.N.J. 1996). That is so for at least three reasons: (1) such an interpretation ignores the plain statutory language that only a *VTSP* can violate the disclosure restrictions, *Daniel v. Cantrell*, 375 F.3d 377, 383 (6th Cir. 2004); *see* § 2710(b)(1); (2) it would render Congress' detailed definition of a VTSP superfluous, *Daniel*, 375 F.3d at 383; and (3) such an expansive prohibition against disclosure would act as a prior restraint of speech, thereby raising serious constitutional questions, *ACLU v. Holder*, 652 F. Supp. 2d 654, 669 (E.D. Va. 2009).

Am. LLC, the court dismissed a VPPA claim against Sony because "plaintiff's allegations fail to state that a disclosure has affirmatively taken place, identify with particularity the person(s) or entity to whom such disclosure was made, or state that any such disclosure falls outside the scope of disclosures permitted under the VPPA." 2012 U.S. Dist. LEXIS 55959, at *3-4 (N.D. Cal. Apr. 20, 2012). For the same reasons, Plaintiffs' disclosure claim should be dismissed.[10]

2. Plaintiffs Fail To Plead A Failure To Destroy Claim

Plaintiffs also allege that Google violated 18 U.S.C. § 2710(e), which requires the destruction of old PII. *See* Compl. ¶ 131. As with their disclosure claim, this claim fails because (1) Google is not a VTSP, and (2) it never collected

---

[10] Plaintiffs' claim also fails because they do not allege facts to demonstrate that PII was ever disclosed to Google. PII is defined as "information which identifies a person as having requested or obtained specific video materials from" a VTSP. 18 U.S.C. § 2710(a)(3). Plaintiffs allege that the URLs of the Viacom websites they visited constitute PII. Compl. ¶¶ 78, 80, 129-30, 139-40. But the only URL they cite, which they claim "identifies the exact title of the video the user has requested and received," provides no such information. *See id.* ¶¶ 80, 78, 140 (discussing http://www.nick.com/shows/penguins-of-madagascar). To the contrary, the URL directs a browser to a webpage containing a variety of games, videos, and information related to a television series called "The Penguins of Madagascar." This webpage is properly considered here because it is incorporated by reference into the complaint. *See, e.g.*, *Edelman v. Croonquist*, 2010 U.S. Dist. LEXIS 43399, at *4, n.1 (D.N.J. May 4, 2010). Even if the URL were disclosed to Google, it does not identify (1) a person, as (2) having requested or obtained *any* video, let alone "*specific* video materials." *See Gonzalez v. Cent. Elec. Coop., Inc.*, No. 08-6240, 2009 U.S. Dist. LEXIS 98104, at *33 (D. Ore. Oct. 15, 2009) (no VPPA violation where VTSP disclosed that the customer rented *a* video, without identifying the specific video). It is not PII.

PII, and therefore could not violate any requirement to destroy PII. The claim also fails because (3) there is no VPPA cause of action for failure to destroy PII, and (4) Plaintiffs have pleaded no facts to support a failure to destroy claim.

i. There Is No Private Right of Action

Based on the text, structure, and purpose of the VPPA, nearly every court to have considered whether § 2710(e), titled "Destruction of Old Records," provides a private right of action agrees that it does not. *See Daniel*, 375 F.3d at 384-85; *Sterk v. Redbox Automated Retail, LLC*, 672 F.3d 535, 538 (7th Cir. 2012) (holding no private cause of action for damages for violation of § 2710(e)); *Rodriguez v. Sony Computer Entm't Am. LLC*, 2012 U.S. Dist. LEXIS 55959, at *2 (N.D. Cal. Apr. 20, 2012) (currently on appeal).

The VPPA's plain language compels this interpretation. While § 2710(b)(1) indicates that a VTSP "shall be liable" for violating the disclosure rule, § 2710(e) contains no similar language concerning a violation of the destruction rule. Moreover, § 2710(c), which discusses the requirements for bringing a "civil action," immediately follows the disclosure provisions of § 2710(b), while § 2710(e) falls two sections below (c). If Congress intended (e) to provide a basis for liability, "it would make sense that the section on civil actions would come at the end of the statute." *Daniel*, 375 F.3d at 384.

A private cause of action only for disclosure claims is also consistent with Congressional intent to provide a remedy only to plaintiffs who are "*aggrieved*." *See* 18 U.S.C. § 2710(c)(1). An "aggrieved" person is one who is injured. *See* Black's Law Dictionary 33 (6th ed. 1990) ("aggrieved" means "having suffered loss or injury"; "injured"). No plaintiff could be injured by the retention of PII, unless it had been wrongfully disclosed. As Judge Posner explained, "[i]f, though not timely destroyed, [PII] remained secreted in the video service provider's files until it was destroyed, there would be no injury." *Sterk*, 672 F.3d at 538.[11]

Here, § 2710(c)—which authorizes a private cause of action for damages and equitable relief—"is limited to enforcing the prohibition of disclosure." *Sterk*, 672 F.3d at 538. Thus, Plaintiffs' § 2710(e) claim should be dismissed.

ii. Google Did Not Retain PII Longer Than Necessary

Plaintiffs' claim should be dismissed for the additional reason that they do not plead facts supporting an allegation that Google retained Plaintiffs' PII more "than one year from the date the information is no longer necessary for the

[11] Lack of a cause of action does not make the destruction requirements of § 2710(e) meaningless. "If the failure to timely destroy such records resulted in harm to the consumer [such as disclosure to a third-party], he could presumably bring a negligence action against the VTSP and benefit from the existence of section (e) by arguing negligence per se." *Daniel*, 375 F.3d at 384 n.5.

purpose for which it was collected." 18 U.S.C. § 2710(e); *Iqbal*, 556 U.S. at 678. Nor could they make such an allegation consistent with their Rule 11 obligations.

F. The New Jersey Computer Related Offenses Act Claim Should Be Dismissed (Count V)

To state a New Jersey Computer Related Offenses Act ("CROA") claim, Plaintiffs must allege Google (1) "damaged [Plaintiffs] in business or property," by (2) engaging in enumerated conduct. N.J.S.A. § 2A:38A-3. These claims "mirror" claims under § 502 of the California Penal Code (the "CCL") (*Joseph Oat Holdings, Inc. v. RCM Digesters, Inc.*, 409 F. App'x 498, 504 (3d Cir. 2010)) and are "similar" to CFAA claims (*Mu Sigma, Inc. v. Affine, Inc.*, 2013 U.S. Dist. LEXIS 99538, at *30 (D.N.J. July 17, 2013)).[12] The CROA has never been applied to ordinary Internet activity of the type Plaintiffs challenge here. Claims

[12] The CCL and CFAA are essentially coextensive. *See Multiven, Inc. v. Cisco Sys., Inc.*, 725 F. Supp. 2d 887, 895 (N.D. Cal. 2010). Both were enacted to combat computer hackers and malicious viruses, not ordinary commercial activity. *WEC Carolina Energy Solutions LLC v. Miller*, 687 F.3d 199, 201, 207 (4th Cir. 2012) ("[C]ourts should not . . . transform[] a statute meant to target hackers into a vehicle for imputing liability to [defendants] who access computers or information in bad faith."); *United States v. Nosal*, 676 F.3d 854, 857-58 (9th Cir. 2012) (en banc) (CFAA is an "anti-hacking statute," not "a sweeping Internet-policing mandate"); *In re Facebook Privacy Litig.*, 2011 U.S. Dist. LEXIS 147345, at *14 & n.8 (CCL not aimed at abuse of a "standard web browser function"); *Integral Dev. Corp. v. Tolat*, 2013 U.S. Dist. LEXIS 153705, at *10 (N.D. Cal. Oct. 25, 2013) (describing CFAA and CCL as "anti-hacking statutes."). The CROA should be interpreted through the lens of that same policy objective. *See Joseph Oat Holdings*, 409 F. App'x. at 503, 504, 506 (describing the CROA as an "anti-hacking statute").

challenging such conduct have been repeatedly rejected under both the CCL and CFAA. *See, e.g.*, *Cookie Litig.*, 2013 U.S. Dist. LEXIS 145727, at *27-32; *In re iPhone Application Litig.*, 2011 U.S. Dist. LEXIS 106865, at *33-41 (N.D. Cal. Sept. 20, 2011); *In re Google Android Consumer Privacy Litig.*, 2013 U.S. Dist. LEXIS 42724, at *21-24, *33-37 (N.D. Cal. Mar. 26, 2013).

1. Google Did Not Damage Plaintiffs in Business or Property

Plaintiffs do not allege that they suffered any Article III injury (*supra* pp. 11-15), much less that Google "damaged [them] in business or property." The CROA damage requirement should be construed as the CFAA's parallel "damage" and "loss" provisions, which establish injury requirements more stringent than Article III.[13] Plaintiffs' generalized allegations about the value of personal information allegedly collected by Google do not meet the requirement.[14]

---

[13] *See Mintel Int'l Grp., Ltd. v. Neergheen*, No. 08-cv-3939, 2010 WL 145786, at *9 (N.D. Ill. Jan. 12, 2010) ("damage" under CFAA limited to "situations in which data is lost or impaired because it was erased or otherwise destroyed, or in which computer networks or databases are disabled"); *iPhone II*, 844 F. Supp. 2d at 1067 ("loss" under CFAA limited to "to the traditional computer 'hacker' scenario-where the hacker deletes information, infects computers, or crashes networks"); *Creative Computing v. Getloaded.com LLC*, 386 F.3d 930, 935 (9th Cir. 2004) ("Only 'economic damages' qualify as 'losses' under the CFAA.").

[14] *Cookie Litig.*, 2013 U.S. Dist. LEXIS 145727, at *28 ("[P]laintiffs have not shown individual economic loss"); *DoubleClick*, 154 F. Supp. 2d at 525 (Plaintiffs "have not pled that DoubleClick caused any damage whatsoever to

(continued...)

2. Google Did not Purposefully or Knowingly Harm Plaintiffs

"[E]ach subsection [of the CROA] requires that the conduct by [Google] be purposeful or knowing." *Fairway Dodge, Inc. v. Decker Dodge, Inc.*, 191 N.J. 460, 469 (2007). Accordingly, Plaintiffs must plead facts showing that Google purposefully or knowingly damaged Plaintiffs in business or property; merely alleging that Google engaged in purposeful conduct is insufficient. Such an interpretation is consistent with the similar requirements of the CFAA.[15] Here, Plaintiffs cannot satisfy this element because their allegations confirm Google's purpose in using cookies was to deliver tailored ads, not to harm Plaintiffs' business or property. *See supra* at pp. 9-10; *DoubleClick*, 154 F. Supp. 2d at 519.

(...continued from previous page)
plaintiffs' computers, systems or data that could require economic remedy."); *Bose v. Interclick, Inc.,* 2011 U.S. Dist. LEXIS 93663, at *15 ("The collection of demographic information does not constitute damage to consumers . . ."). Plaintiffs' failure to plead any cognizable "damage" defeats their CROA claim. *Fairway Dodge, Inc. v. Decker Dodge, Inc.*, 2006 N.J. Super. Unpub. LEXIS 1360, at *28 (App. Div. June 12, 2006) ("[L]iability is established only if [plaintiff] has been damaged in business or property.").

[15] *See Kalow & Springnut, LLP v. Commence Corp.*, 2008 U.S. Dist. LEXIS 48036, at *9 (D.N.J. June 23, 2008) ("alleg[ation] that [defendant] intentionally transmitted a software code to [plaintiff]'s computer system and that, the software code . . . caused damage to them" insufficient to plead intentional harm under the CFAA); *Oracle Corp. v. SAP AG*, 734 F. Supp. 2d 956, 964 (N.D. Cal. 2010) ("[P]laintiffs must allege and prove that [the defendant] specifically 'intended' to 'cause damage'").

3. Plaintiffs Cannot Satisfy the Remaining Elements Required for the Subsections of the CROA

Plaintiffs do not allege facts to satisfy any of the CROA's subsections:

- *CROA subsections 3(a)-(b)*. Plaintiffs do not allege a subsection 3(a)-(b) claim because Google merely communicated with their browsers as the browsers were designed to communicate, without causing any alteration, damage, or taking. The only data Google obtained by placing cookies on Plaintiffs' browsers was data it had permission to access: its cookie values. *See supra* at pp. 20-22; *PNC Mortg. v. Superior Mortg. Corp.*, 2012 U.S. Dist. LEXIS 25238, at *14 (D.N.J. Feb. 27, 2012) (dismissing CROA claim;"there are no facts that show that any data or information was taken. . ."); *P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504, 509 (3d Cir. 2005) (same).

- *CROA subsection 3(c)*. Plaintiffs cannot state a subsection 3(c) claim because they cannot show that Google engaged in unauthorized access. *First*, Plaintiffs voluntarily sent GET commands to Google. *Second*, the only data Google obtained by placing cookies on Plaintiffs' browsers were the values of Google's own cookies. *Third*, Plaintiffs fail to plead facts supporting an inference that Google *hacked* their computers. The term "access" is defined by section 2A:38A-1(a) "in terms redolent of 'hacking' or breaking into a computer," which "is different from the ordinary, everyday use of a computer." *Chrisman v. City of Los Angeles*, 65 Cal. Rptr. 3d 701, 704-05 (Cal. Ct. App. 2007);[16] *see also Joseph Oat Holdings*, 409 F. App'x. at 503, 504, 506 (describing the CROA as an "anti-hacking statute"); *P.C. Yonkers*, F.3d 428 at 509 (finding that the CROA "require[s] proof of some activity vis-a-vis the information other than simply gaining access to it"). Because Google was authorized to communicate with

---

[16] While *Chrisman* interpreted the CCL, the CROA defines the term "access" similarly and should therefore be interpreted similarly. *Compare* N.J. Stat. § 2A:38A-1(a) ("'Access' means to instruct, communicate with, store data in, retrieve data from, or otherwise make use of any resources of a computer, computer system, or computer network.") *with* Cal. Pen. Code § 502(b)(1) ("'Access' means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory function resources of a computer, computer system, or computer network."); *see also supra* p. 33 & n.12; *Smith v. City of Jackson, Miss.*, 544 U.S. 228, 233 (2005).

Plaintiffs' browsers, *see supra* pp. 17-20, 27, Plaintiffs' allegations do not support an inference of hacking.

- *CROA* subsection *3(d)*. Subsection (d) is inapplicable to Plaintiffs' allegations because it only applies to "financial instrument[s]."

- *CROA* subsections *3(e)*. Plaintiffs' subsection (e) claim fails because, as discussed above, they do not plead facts that Google hacked their computers.

G. The Intrusion Claim (Count VI) Should Be Dismissed

Plaintiffs do not specify whether their intrusion claim (Count VI) is based on California or New Jersey law.[17] Compl. ¶¶ 194-97. Regardless, the claim fails because Plaintiffs have not alleged that Google (1) intentionally (2) invaded a legally private matter (3) in a manner "highly offensive to a reasonable person." *Hennessey v. Coastal Eagle Point Oil Co.*, 129 N.J. 81, 94-95 (1992) (quoting Restatement (Second) of Torts, § 652B (1977)); *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 992 (Cal. Ct. App. 2011) (same).

1. Google Lacked the Requisite Intent

First, Plaintiffs do not allege Google had the requisite intent. "[A]n actor commits an intentional intrusion only if he believes, or is substantially certain, that he lacks the necessary legal or personal permission to commit the intrusive act."

---

[17] This omission alone warrants dismissal. *Cf. In re Ductile Iron Pipe Fittings (DIPF) Indirect Purchaser Antitrust Litig.*, No. 12-169, 2013 U.S. Dist. LEXIS 142466, at *25 (D.N.J. Oct. 2, 2013) ("*DIPF Litig.*"). Despite this failing, however, it is possible to evaluate (and reject) Plaintiffs' intrusion claim because, as explained *supra*, California and New Jersey law are consonant in this area.

O'Donnell v. United States, 891 F.2d 1079, 1083 (3d Cir. 1989); *accord Dubbs v. Head Start, Inc.*, 336 F.3d 1194, 1221 (10th Cir. 2003). Plaintiffs do not allege Google knew it was violating the law by placing cookies on their browsers (and it was not). Google's intent "has plainly not been to perpetuate torts" but to "make money by providing a valued service." *DoubleClick*, 154 F. Supp. 2d at 519.

2. Google Did not Invade a Legally Private Matter

Second, Plaintiffs fail to allege that Google invaded a private matter. The communications between Plaintiffs' browsers and the websites were not "private": Google was party to them and would have been regardless of the cookies. *Supra* at pp. 7-9, 17-20; *Cookie Litig.*, 2013 U.S. Dist. LEXIS 145727, at *33 ("[T]ransfer of inputted information . . . would have occurred regardless of Google's placement of cookies"); *see also Poltrock v. NJ Auto. Accounts Mgmt. Co.,* 2008 U.S. Dist. LEXIS 103351, at *18-19 (D.N.J. Dec. 22, 2008) ("voluntar[y] disclos[ure]" of information "waives a plaintiff's privacy interest entirely"). Moreover, Google obtained no "private" information because the only additional information Google received was the value of its cookies, which were previously known to Google. *Supra* at pp. 9-10; *see also Poltrock*, 2008 U.S. Dist. LEXIS 103351, at *12-21 (dismissing intrusion claim arising from information already known to defendant).

3. The Alleged Intrusion Was not Highly Offensive

Third, Plaintiffs fail to establish that the alleged intrusion was highly offensive to a reasonable person. Google's alleged receipt of information sent to it

by Plaintiffs' browsers and use of cookies to correlate it to display tailored ads does not satisfy this "high bar" (*Low*, 900 F. Supp. 2d at 1025), especially since this practice is long-standing, well-known, ubiquitous, and fundamental to Internet services. *See* Compl. ¶¶ 32-48; *supra* pp. 6-7. Not surprisingly, *Cookie Litig.* reached the same conclusion concerning substantively identical allegations. 2013 U.S. Dist. LEXIS 145727, at *33-34; *see also Low*, 900 F. Supp. 2d at 1025-26 (disclosure of browsing history not highly offensive); *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).

H. The Unjust Enrichment Claim Should Be Dismissed (Count VII)

The Complaint alleges an unjust enrichment claim (Count VII) without invoking any state law. Compl. ¶¶ 198-201. This failure requires dismissal. *DIPF Litig.*, 2013 U.S. Dist. LEXIS 142466, at *25. Even on the merits, Plaintiffs' claim fails. Under California law, unjust enrichment "is not a cause of action, just a restitution claim." *Hill v. Roll Int'l Corp.*, 195 Cal. App. 4th 1295, 1307 (Cal. Ct. App. 2011); *Low*, 900 F. Supp. 2d. at 1031. New Jersey "does not recognize unjust enrichment as an independent tort cause of action." *Castro v. NYT Television*, 370 N.J. Super. 282, 299 (App. Div. 2004). It is "a quasi-contractual claim" that is dismissed where, as here, "Plaintiff [has not] conferred a benefit upon Defendants, [] expected remuneration from Defendants, or . . . had a quasi-contractual

relationship with Defendants." *Mu Sigma*, 2013 U.S. Dist. LEXIS 99538, at *32-34 & n.8.

CONCLUSION

For the foregoing reasons, Google respectfully requests that the Complaint be dismissed.

.

Respectfully submitted,

SILLS CUMMIS & GROSS P.C.
One Riverfront Plaza
Newark, New Jersey 07102-5400
Telephone: (973) 643-7000

By: */s/ Jeffrey J. Greenbaum*
Jeffrey J. Greenbaum
jgreenbaum@sillscummis.com

Colleen Bal
(admitted *pro hac vice*)
Michael H. Rubin
(admitted *pro hac vice*)
WILSON SONSINI GOODRICH & ROSATI, P.C.
One Market Plaza
Spear Tower, Suite 3300
San Francisco, CA 94105-1126
Telephone: (415) 947-2000
cbal@wsgr.com
mrubin@wsgr.com

Attorneys for Defendant Google Inc

Dated: January 15, 2014