No. 15-1441

IN THE

United States Court of Appeals

FOR THE THIRD CIRCUIT

IN RE: NICKELODEON CONSUMER PRIVACY LITIGATION

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEW JERSEY

ANSWERING BRIEF OF DEFENDANT-APPELLEE GOOGLE INC.

COLLEEN BAL
MICHAEL H. RUBIN
WILSON SONSINI GOODRICH & ROSATI
PROFESSIONAL CORPORATION
One Market Street, Spear Tower,
Suite 3300
San Francisco, California 94105
(415) 947-2000

Counsel for Defendant-Appellee Google Inc.

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1, Defendant-Appellee Google Inc. certifies that it has no parent corporation and that no publicly-held corporation owns 10% or more of its stock.

Dated: June 15, 2015 /s/ Colleen Bal

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

RULES

MISCELLANEOUS

TABLE OF ABBREVIATIONS

A___	Citations to the Appendix on Appeal
CFAA	Computer Fraud and Abuse Act, 18 U.S.C. § 1030
CIPA	California Invasion of Privacy Act, Cal. Penal Code § 631
CROA	New Jersey Computer Related Offenses Act, N.J. Stat. Ann. §§ 2A:38A-1 to -6
Defendants	Defendants-Appellees Google Inc. and Viacom, Inc.
Google	Defendant-Appellee Google Inc.
MCC	Master Consolidated Class Action Complaint
MCC Order	July 2, 2014 Opinion dismissing MCC, A6-44
PII	Personally Identifiable Information
Plaintiffs	Plaintiffs-Appellants
POB	Plaintiffs-Appellants' Opening Brief on Appeal
Pls.' Opp.	Plaintiffs' Opposition to Defendants' Motions to Dismiss (Dkt. No. 52)
SAC	Second Consolidated Class Action Complaint
SAC Order	January 20, 2015 dismissing SAC, A47-57
SCA	Stored Communications Act, 18 U.S.C. § 2701
VPPA	Video Privacy Protection Act, 18 U.S.C. § 2710
Wiretap Act	Electronic Communication Privacy Act, 18 U.S.C. § 2511

INTRODUCTION

This multidistrict litigation consists of six consolidated actions brought on behalf of putative nationwide classes of individuals who allege that when they visited certain Viacom websites, Google placed cookies on their browsers. Cookies are a standard feature of the modern Internet used for a host of legitimate purposes. The only result of the cookie placement alleged by Plaintiffs was that more relevant ads might have been displayed in Plaintiffs' browsers than the ads that would otherwise have been shown. That could not have harmed Plaintiffs. Accordingly, they lack standing. In addition, Plaintiffs fail to state a claim under the statutory or common law theories they advance. For these reasons, the District Court properly dismissed this action, and that ruling should be affirmed.

COUNTERSTATEMENT OF JURISDICTION

Google agrees that this Court has jurisdiction over the appeal pursuant to 28 U.S.C. § 1291. As discussed in Part I below, however, the District Court did not have subject matter jurisdiction because Plaintiffs suffered no injury-in-fact and therefore lack standing to pursue this action under Article III of the United States Constitution.

COUNTERSTATEMENT OF THE ISSUES

1. Should the Court affirm the District Court's dismissal of claims against Google on the alternative ground that the Court lacks subject matter jurisdiction because Plaintiffs allege no overpayment of money, no expenses incurred, no lost profits, or any other actual injury resulting from Google's alleged placement of cookies on their browsers?

2. Should the Court affirm the District Court's dismissal of Plaintiffs' Wiretap Act claim because (a) Google did not intercept the "contents" of any communications, (b) Google was a party to the communications at issue and Viacom consented to Google's receipt of these communications, and (c) Plaintiffs did not plausibly allege that Google illegally intercepted the communications of "other websites"?

3. Should the Court affirm the District Court's dismissal of Plaintiffs' California Invasion of Privacy Act ("CIPA") claim because (a) Google is a party to the communications at issue in this case, and (b) Plaintiffs did not allege the interception of the "content or meaning" of a protected communication?

4. Should the Court affirm the District Court's dismissal of Plaintiffs' Stored Communications Act ("SCA") claim because (a) cookies

allegedly placed on Plaintiffs' browsers did not enable Google to "obtain" Plaintiffs' communications, (b) Plaintiffs' personal devices and browsers are not "facilities" of an "electronic communications service," and (c) Google did not access any communications in "electronic storage"?

5. Should the Court affirm the District Court's dismissal of Plaintiffs' Video Privacy Protection Act ("VPPA") claim because (a) Google is not a "video tape service provider," and (b) Google did not disclose Plaintiffs' personally identifiable information ("PII")?

6. Should the Court affirm the District Court's dismissal of Plaintiffs' New Jersey Computer Related Offenses Act ("CROA") claim because (a) Google's alleged placement of cookies on Plaintiffs' browsers did not damage Plaintiffs in business or property, (b) Plaintiffs did not allege prohibited conduct, and (c) Google did not purposefully or knowingly harm Plaintiffs?

7. Should the Court affirm the District Court's dismissal of Plaintiffs' intrusion upon seclusion claim because (a) Google did not invade a legally private matter, (b) Google's alleged conduct was not highly offensive, and (c) Google neither believed nor was substantially cer-

tain that it lacked the necessary legal or personal permission to allegedly place cookies on Plaintiffs' browsers?

COUNTERSTATEMENT OF RELATED CASES

This case has not come before this Court previously. Google knows of no other related case or proceeding. While there is no direct relationship between this case and *In re Google Cookie Placement Consumer Privacy Litigation*, No. 13-4300, the two cases raise similar questions under the Wiretap Act, SCA, and CIPA.

COUNTERSTATEMENT OF THE CASE

This litigation challenges Google's use of Internet "cookies" that help Google deliver ads to computer users who visit Viacom's Nickelodeon websites. Like many website operators, Viacom employs Google's advertising services to display ads to visitors to its websites. Google uses "DoubleClick ID cookies" to deliver those ads. Plaintiffs admit that Viacom invited Google to place these cookies. They further admit that when they visited Viacom's websites, Plaintiffs voluntarily sent to Google the supposed "personal information" at issue as part of the routine operation of the Internet. And they admit still further that they would have transmitted that same information to Google whether or not

Google's cookies were present on their browsers.

A. HOW BROWSERS INTERACT WITH WEBSITES

The layout of most webpages includes multiple components, such as text, pictures, videos, ads, and other material. A113, 116-17. When a computer user visits a webpage by typing a web address (or "URL") into a browser or clicking a website link, the user's browser sends a so-called "GET" request asking the website for instructions to load the webpage. A112-13; *see also* POB at 35. The GET request includes certain information generated by the browser, such as the browser version and operating system, that enables the website to display the requested information. A63-66, 68-69, 79-80, 94, 112-13, 116-17, 128-30.

The website responds to the GET request by telling the browser where and, if necessary, from which third parties to retrieve the material that makes up the webpage—the text, pictures, videos, links, and ads. A113, 116-17. For example, a particular page on a website may contain text and pictures hosted on that website, as well as an ad from one third-party site and another ad from a different third-party site. A114. Once the browser knows where to go to get the full complement of material that will make up the webpage, the browser sends additional

GET requests to any third parties (such as Google) that have the material, telling those third parties which webpage the browser is trying to load, requesting the relevant information, and providing the same information that the browser gave to the original website. A113, 116-17.

Equipped with the information that the user's browser provides, the relevant third parties can send back the appropriate material. *See* A113, 117; POB at 36 ("Plaintiffs also receive information in response to those GET requests"). The webpage the user requested cannot be properly displayed unless third parties like Google receive this information from a user's GET request(s) and send the information back to the user's browser. A113, 116-17. This back-and-forth between browsers, websites, and third parties is a standard and essential function of the Internet.

The information generated and sent by Plaintiffs' browsers—including the URL of the websites they are visiting and the other information Plaintiffs allege is "personal information"—is provided *voluntarily* to websites and third parties like Google in GET requests before the websites or third parties ever send any communications back to Plaintiffs' browsers. A112-13, 116-17; POB at 35-36. Indeed, Plaintiffs

characterize this transmission of information as not merely voluntary, but as a "deliberate act[]" and "conscious choice by the user." POB at 35. This process is what enables Internet users to access the websites they request to see, including the advertisements displayed on those sites.

B. GOOGLE'S USE OF THE DOUBLECLICK ID COOKIE TO SERVE BETTER ADS

Cookies have come to be a "ubiquitous" online technology that "plays a large role in Internet users' Web browsing." *Netscape Commc'ns Corp. v. ValueClick, Inc.*, 684 F. Supp. 2d 678, 682 (E.D. Va. 2009). Cookies are small text files that are transmitted between a website and an Internet browser; "persistent" cookies, such as those at issue here, remain stored on the browser until their set expiration time. A67, 114; *see also In re Google Inc. Cookie Placement Consumer Privacy Litig.* ("*Cookie Litig.*"), 988 F. Supp. 2d 434, 439 (D. Del. 2013). Cookies are "widely used on the Internet by reputable websites to promote convenience and customization." *In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d 9, 14 (1st Cir. 2003); *see* A114-16.

Cookies are useful in Internet advertising for a variety of reasons. They help prevent fraud; they can measure the results of a given advertising campaign; and most notably here, they allow for the display of

ads that are more relevant to the viewer. A116, 118. The Google advertising cookie (the DoubleClick ID cookie) has been in use for more than a dozen years. *See* A131; *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 504 (S.D.N.Y. 2001). As the District Court here noted, this cookie enables Google to target advertising to Plaintiffs based upon "Plaintiffs' 'individualized web usage.'"[1] A8-9 (October 23, 2013 order dismissing MCC ("MCC Order")); *see also* A48 (January 20, 2015 order dismissing SAC ("SAC Order")).

When a user requests a webpage on one of the Nickelodeon websites at issue, the user's browser sends GET requests to Viacom and to Google. A112-13, 116-17. If a DoubleClick ID cookie has already been set on the user's browser, then as part of the GET request, the browser sends Google's server the cookie value—an alphanumeric number as-

[1] Plaintiffs' opening brief makes the unsupported allegation "upon information and belief" that Viacom "procured" Google to track Plaintiffs' browsing activities so that Viacom could sell more ads on its sites targeted to Plaintiffs, and thereby profit from Google's targeted advertising. POB at 8. This allegation is not part of the complaint and was never asserted below; the SAC (A116) merely alleges that companies such as Defendants have ways of monetizing cookies.

signed to the cookie by Google. *See* A116-18.[2] The DoubleClick ID cookie does not collect information from Internet users, and Plaintiffs do not allege that it does. *See* A116-18. Instead, the cookie value allows Google to recognize that a browser visiting a webpage displaying a Google ad is the same browser as one that has previously visited other webpages displaying Google ads. Google can then *organize* the information from the user's visits—information that the user is *already sending* to Google in his or her GET requests. A116-18; *DoubleClick*, 154 F. Supp. 2d at 503. As the District Court recognized, the cookie text file simply "assign[s] to each Plaintiff an identifier that is associated with other information" that Google "use[s] … to target Plaintiffs with advertising." A48. The cookie's presence thus enables Google to present more relevant ads to the browser the next time the browser visits a webpage that employs Google's ad services. *See* A115-16, 118; *DoubleClick*, 154 F. Supp. 2d at 505; *see also Cookie Litig.*, 988 F. Supp. 2d at 439-40; *Pharmatrak*, 329 F.3d at 14.

[2] If the user's browser does not have a DoubleClick ID cookie already set, Google sends a cookie to the browser as part of its response to the GET request. A114, 117.

Plaintiffs concede that their browsers send the same information to the websites they access and to Google's advertising system *regardless of whether a DoubleClick ID cookie is present*. A112-13, 116-17, 128-29; *see also* Pls.' Opp. to Defs.' Mots. to Dismiss at 34 (Dkt. No. 52) ("Pls.' Opp.") ("Google would still receive URLs in the form of GET requests"); *Cookie Litig.*, 988 F. Supp. 2d at 443 ("[P]laintiffs' browsers voluntarily sent to Google the information inputted by plaintiffs [as part of the GET request], regardless of whether plaintiffs' browsers had any Google cookies set."); *id.* at 444 ("[P]laintiffs' browsers would send a URL [to Google as part of the GET request] regardless of whether a third party cookie was set."). Plaintiffs do not allege that any additional or different information is sent from their browsers to Google when a DoubleClick ID cookie is present than when no cookie is present, other than the (Google-created) cookie value itself. *See* A117-18.

C. PROCEDURAL BACKGROUND

In 2012, Plaintiffs filed six federal civil actions against Viacom and Google in federal courts across the country. The Judicial Panel for Multidistrict Litigation then transferred these actions to the District of New Jersey for coordination in June 2013. Aplts.' Addendum to App'x.

at 9 (Dkt. # 003111958964). The District Court consolidated these actions, and Plaintiffs filed their Master Consolidated Class Action Complaint (the "MCC") in October 2013. A59-107. The MCC asserted various federal and state claims against Google and Viacom on behalf of two putative classes: (1) a "U.S. Resident Class" of "All 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"; and (2) a "Video Subclass" of "All 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." A83-84.

Google and Viacom each filed motions to dismiss. The District Court granted those motions and dismissed the MCC under Rule 12(b)(6). A44. The Court dismissed with prejudice the VPPA claim against Google because Google is not a video tape service provider ("VTSP") under the VPPA. A15-20. The Court also dismissed the VPPA claim against Viacom, albeit with leave to amend, because the infor-

mation allegedly transmitted by Viacom to Google did not constitute personally identifiable information ("PII"). A25-26, 28-29.

The Court also held that the same information—including IP addresses and URLs—did not constitute "contents" as required to state a claim under the Wiretap Act or the CIPA, and therefore also dismissed these claims with prejudice. A33-36. In dismissing the Wiretap Act claim, the District Court also recognized that "all communications in this case were either directly between [Defendants] (or their cookies) and Plaintiffs' computers, or intercepted with the express consent of websites like Viacom." A31. Finally, the Court dismissed Plaintiffs' SCA and unjust enrichment claims with prejudice and their CROA and intrusion upon seclusion claims without prejudice. A36-38, 40-44.[3]

Plaintiffs filed their Second Consolidated Class Action Complaint (the "SAC") in September 2014, on behalf of the same U.S. Resident Class and Video Subclass, except with respect to only one Nickelodeon

[3] Because it allowed Plaintiffs leave to amend on certain "claims for violations of statutes that codify certain of their privacy rights," the District Court did not dismiss the action under Rule 12(b)(1) for lack of standing under Article III, despite acknowledging its "doubts about whether [Plaintiffs] have suffered concrete monetary harm." A13.

website (Nick.com) rather than the original three. A108-62. Defendants again moved to dismiss, and the District Court granted the motions, this time with prejudice as to all claims. A47.

The Court explained that Plaintiffs' amended allegations still failed to plausibly allege "that the information collected does indeed identify Plaintiffs" "*without more*," so it was irrelevant whether Google could theoretically combine information from its other services to "ascertain personal identities." A51. The Court recognized that Google did not allow children like Plaintiffs who are under age 13 to register for its services as "is necessary for the theoretical combination of information to actually yield one of the Plaintiff's identities." A51-53. The Court determined that Plaintiffs' new allegations still failed to allege "business or property" damage under the New Jersey CROA, A53-54, and held that Defendants' "collection and disclosure of anonymous browsing history and other similar information" is not "highly offensive" to state a claim for intrusion upon seclusion. A54-57. This appeal followed.

COUNTERSTATEMENT OF THE STANDARD OF REVIEW

The Court reviews *de novo* the dismissal of a complaint under Rule 12 of the Federal Rules of Civil Procedure. *Ballentine v. United*

States, 486 F.3d 806, 808 (3d Cir. 2007). While the Court may affirm on any ground supported by the record, it does not consider an appellant's arguments if they were not presented to the District Court, *United States v. Joseph*, 730 F.3d 336, 342 (3d Cir. 2013), nor will it consider any arguments not raised in the appellant's opening appeal brief, *see Laborers' Int'l Union of N. Am. v. Foster Wheeler Corp.*, 26 F.3d 375, 398 (3d Cir. 1994).[4]

SUMMARY OF THE ARGUMENT

Standing. The Court should affirm the dismissal of Plaintiffs' claims because Plaintiffs suffered no Article III injury as a result of the alleged placement of cookies on their browsers. The only possible effect that the presence of Google's cookies had on Plaintiffs was to cause the display of a different advertisement than the one that otherwise might have been displayed. That is not an injury-in-fact.

Failure to State a Claim. The Court should also affirm the dismissal of each of Plaintiffs' claims under Rule 12(b)(6).

[4] Google addresses the proper standards for dismissing a complaint under Rules 12(b)(1) and 12(b)(6) at the beginning of Section I and Section II, respectively. *Infra* pp. 17, 23.

- **Wiretap Act/CIPA**. These statutes prohibit the intentional interception of the contents of communications by persons who are not parties to the communications. 18 U.S.C. § 2511(2)(d). Plaintiffs claim that Google used the DoubleClick ID cookie to intercept their communications, but concede that the only communications Google obtains other than the value assigned by Google to the cookie are communications that Plaintiffs intentionally transmitted to Google through GET requests. Google is a party to the communications and thus cannot be charged with improperly intercepting them under the Wiretap Act or CIPA. Those claims fail for the additional reason that Google did not receive the "contents" of Plaintiffs' communications, *i.e.* "information concerning the substance, purport or meaning of th[e] communication," as a result of the cookies. 18 U.S.C. § 2510(8); Cal. Penal Code § 631. The only information Plaintiffs allege Google received by virtue of the cookies—the cookie value itself—is not "contents" for purposes of the wiretapping laws. *See* A117-18.

- **SCA**. This statute 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). Plaintiffs' claim fails because (i) cookies allegedly placed on Plaintiffs' browsers did not enable Google to "obtain" Plaintiffs' communications, (ii) Plaintiffs' personal devices and browsers are not "facilities" of an "electronic communications service," and (iii) Google did not access any communications in "electronic storage."

- **VPPA**. This statute prohibits knowing disclosures by a "video tape service provider" ("VTSP") of "information that identifies a person as having requested or obtained specific video materials from a VTSP." Plaintiffs' 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.

- **New Jersey CROA**. This claim 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.

- **Intrusion on Seclusion**. Plaintiffs' claim fails because (i) assuming counterfactually that placing cookies on Plaintiffs' browsers was unlawful, Plaintiffs allege no facts showing that Google knew and intended such illegality, (ii) Google obtained no private information

from Plaintiffs as a result of its actions, and (iii) the alleged intrusion was not highly offensive because cookies are standard, well known, and fundamental to the provision of countless Internet services.

ARGUMENT

I. PLAINTIFFS LACK ARTICLE III STANDING

"Absent Article III standing, a federal court does not have subject matter jurisdiction to address a plaintiff's claims, and they must be dismissed." *McCray v. Fid. Nat'l Title Ins. Co.*, 682 F.3d 229, 243 (3d Cir. 2012) (citation omitted). "[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, 180-81 (2000). "In the class action context, that requirement must be satisfied by at least one named plaintiff." *McNair v. Synapse Grp. Inc.*, 672 F.3d 213, 223 (3d Cir. 2012) (citing *Warth v. Seldin*, 422 U.S. 490, 502 (1975)).

In this case, the District Court correctly held that Plaintiffs had not alleged any facts showing an actual injury, but the Court nevertheless concluded that standing existed based simply on Plaintiffs' claim that Google violated certain statutes. The Court's ruling that a statutory violation, by itself, creates Article III standing was incorrect, and this Court can and should affirm the dismissal with prejudice on the alternative ground that Plaintiffs do not have standing to pursue their claims against Google. *See Tourscher v. McCullough*, 184 F.3d 236, 240 (3d Cir. 1999) (the Court may affirm the district court on any ground supported by the record).

A. PLAINTIFFS ALLEGE NO ACTUAL INJURY

1. Plaintiffs Allege No Facts Showing Economic Injury

Plaintiffs allege no facts suggesting that the named plaintiffs suffered any personal economic injury resulting from the placement of cookies on their browsers. They allege no overpayment of money, no expenses incurred, no loss of profits, or any other actual economic injury. Plaintiffs cannot satisfy Article III merely by claiming that they "have suffered damages" where there is no factual support for that in the

Complaint. *Storino v. Borough of Point Pleasant Beach*, 322 F.3d 293, 296 (3d Cir. 2003).

Plaintiffs instead make some vague assertions about the value of their personal information. A118-22. But it is well settled that Article III standing does not exist based on speculative allegations that the value of "personal information" was diminished by its collection and use. *See, e.g.*, A12 ("'[w]e are not aware of any court that has held the value of this collected information constitutes damage to consumers or unjust enrichment to collectors'") (quoting *In re DoubleClick*, 154 F. Supp. 2d 497, 525 (S.D.N.Y. 2001)); *LaCourt v. Specific Media, Inc.*, No. 10-1256, 2011 WL 1661532, at *5 (C.D. Cal. Apr. 28, 2011); *Del Vecchio v. Amazon.com Inc.*, No. 11-366, 2011 WL 6325910, at *6 (W.D. Wash. Dec. 1, 2011). As the District Court explained, this theory is akin to "the belief that a football fan could sell her eyeballs to a TV network for four cents because an advertiser pays $4 million to reach 100 million viewers during the Super Bowl." A12.

Plaintiffs here do not allege that anyone was willing to pay them specifically for their limited, anonymous, individual browsing history allegedly obtained by Google. Nor do they allege that they attempted to

sell that information and were unable to do so because of Google's alleged actions. While Plaintiffs make several allegations about the purported quantifiable value of *other* types of information related to online activities (A71-74; 118-22), they identify no lost opportunity to sell their history of visiting websites—the information at issue here. That is not enough for Article III standing.

2. Plaintiffs' Bare Assertion That Their Privacy Was Invaded Does Not Demonstrate Actual Injury

Plaintiffs argued below that their bare allegation of an invasion of privacy creates standing. But this Court squarely rejected any such claim in *Reilly v. Ceridian Corp*. 664 F.3d 38, 40-44 (3d Cir. 2011). There, a hacker infiltrated the defendant's computer system and potentially gained access to the plaintiffs' personal and financial information. The Court held that to establish standing to bring a claim, Article III requires a plaintiff to plead factual allegations showing an actual "detriment" to the plaintiff resulting from the alleged invasion. *Id.* Plaintiffs have not alleged any such detriment here.

B. Plaintiffs' Assertion of a Statutory Violation Does Not Create Injury-in-Fact Under Article III

Having rejected Plaintiffs' cursory efforts to plead that they suffered an actual freestanding injury from Google's actions, the District Court ruled that an alleged violation of a statute, without more, is sufficient to establish Article III standing. That holding is mistaken.

Because an injury in fact is an "irreducible constitutional minimum of standing," *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992), Congress cannot "erase" this requirement by enacting a statute that does not require a plaintiff to prove an injury in fact, *Raines v. Byrd*, 521 U.S. 811, 820 n.3 (1997). Thus, even when Congress "grant[s] an express right of action … Art. III's requirement remains: the plaintiff still must allege a distinct and palpable *injury* to himself." *Warth v. Seldin*, 422 U.S. 490, 501 (1975) (emphasis added).

This Court has been of two minds on the question of statutory standing. Previously, this Court held that plaintiffs must allege an actual injury—not just a violation of a federal statute—to establish Article III standing. *See Fair Housing Council v. Main Line Times*, 141 F.3d 439, 443-44 (3d Cir. 1998) ("a violation of the Act does not automatically

confer standing on any plaintiff"); *Doe v. Nat'l Bd. of Med. Exam'rs*, 199 F.3d 146, 153 (3d Cir. 1999) ("The proper analysis of standing focuses on whether the plaintiff suffered an actual injury, not on whether a statute was violated.").

In ruling otherwise, the District Court relied on a series of this Court's more recent decisions holding that a statutory violation even in the absence of actual injury is sufficient to establish Article III standing. *See* A12-13 (citing *Pichler v. UNITE*, 542 F.3d 380, 390 (3d Cir. 2008); *Alston v. Countrywide Financial Corp.*, 585 F.3d 753, 763 (3d Cir. 2009); *Baldwin v. Univ. of Pittsburgh Med. Ctr.*, 636 F.3d 69, 73 (3d Cir. 2011)). Under Third Circuit law, these more recent decisions do not control because "'[t]his Circuit has long held that if its cases conflict, the earlier is the controlling authority and the latter is ineffective as precedents.'" *Pardini v. Allegheny Intermediate Unit*, 524 F.3d 419, 426 (3d Cir. 2008) (quoting *United States v. Rivera*, 365 F.3d 213, 213 (3d Cir. 2004)).

Recognizing a circuit split on the question of whether a claim of statutory violation can be sufficient to establish Article III standing, the Supreme Court has recently joined the issue by granting certiorari in a

case that presents this very question. *See Spokeo, Inc. v. Robins*, No. 13-1339, 2015 U.S. Dist. LEXIS 2947 (U.S. Apr. 27, 2015). Rather than proceed with this case under circumstances where the Supreme Court may decide this potentially dispositive issue imminently, Google requests that this Court stay its ruling until after the ruling in *Spokeo*. If this Court nevertheless wishes to proceed, the District Court's decision should be affirmed on the merits for the reasons set forth below.

II. PLAINTIFFS FAIL TO STATE A LEGALLY VIABLE CLAIM AGAINST GOOGLE

"[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) (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556 (2007)). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.* at 678. Similarly, the court must "disregard 'naked assertions devoid of further factual enhancement.'" *Santiago v. Warminster Twp.*, 629 F.3d 121, 131 (3d Cir. 2010) (quoting *Iqbal*, 556 U.S. at 678).

Accordingly, while the Court accepts as true all material allegations in the complaint, it need not accept the truth of conclusory allegations or unwarranted inferences, nor should it accept legal conclusions

as true merely because they are cast in the form of factual allegations. *Iqbal*, 556 U.S. at 678-79; *Santiago*, 629 F.3d at 131-33. Courts are to decide a motion to dismiss "not upon the presence of mere words" in the complaint, "but, rather, upon the presence of a factual situation which is or is not justiciable," and will draw on the complaint's allegations "in a realistic, rather than a slavish, manner." *Pearson v. Tanner*, 513 F. App'x 152, 154 (3d Cir. 2013) (quoting *Doug Grant, Inc. v. Greate Bay Casino Corp.*, 232 F.3d 173, 184 (3d Cir. 2000)).

The District Court correctly applied these standards to dismiss each of Plaintiffs' claims. While Plaintiffs' brief—like their Complaint—is filled with conclusory accusations and rhetoric, the facts alleged demonstrate that Plaintiffs have no viable claim against Google.

A. PLAINTIFFS CANNOT STATE A WIRETAP CLAIM

The District Court held that Plaintiffs failed to state a Wiretap Act claim. That ruling should be affirmed for several independent reasons.

1. Plaintiffs Cannot Allege the Interception of "Contents" Protected by the Wiretap Act

First, Plaintiffs cannot identify any "contents" of their communications that were unlawfully intercepted. The Wiretap Act protects only the "contents" of a communication, defined as "information concerning the substance, purport, or meaning of" a communication. 18 U.S.C. §§ 2510(4), (8). "Contents" is "information the user intended to communicate, such as the spoken words of a telephone call." A33 (quoting *Google Litig.*, 2013 U.S. Dist. LEXIS 145727, at *4 & citing *United States v. Reed*, 575 F.3d 900, 916 (9th Cir. 2009)). To be actionable, moreover, those contents must be acquired through the use of an "electronic, mechanical, or other device." 18 U.S.C. § 2510(4) (emphasis added). Here, the only "device" Plaintiffs allege is Google's cookies. A93-94, 97. But Google's cookies do not acquire the contents of Plaintiffs' communications.

The only data that was sent to Google via the DoubleClick ID cookies was the cookie values themselves. A69, 70. Plaintiffs do not allege that these cookie values contained the "contents" of any communication. That is for good reason: as Plaintiffs allege, the cookies are simp-

ly an anonymous string of numbers and letters. A70, 82-83; *DoubleClick*, 154 F. Supp. 2d at 513 (cookie id number is "meaningless to anyone" other than Google).[5] Instead, Plaintiffs only contend that the URLs of the websites visited by Plaintiffs' browsers and Plaintiffs' birthdate and gender are the contents of their communications. POB at 29-37. This argument is a red herring: the alleged transmission of URLs, birthdate, and gender data to Google has nothing to do with the cookies at issue.[6]

---

[5] The addition of the cookie value to the data Plaintiffs otherwise send to Google does not convert the cookie value into "contents" or otherwise alter the analysis. For instance, the email address and date on a blank email are not contents; they are quintessential subscriber information. They do not become contents just because the sender sends a second email, but this time with a lengthy discussion in the body of the email. Similarly here, cookie values do not become contents just because they are allegedly sent with URLs and other information that Plaintiffs claim are contents.

[6] Moreover, as the District Court found, birthdate and gender data is irrelevant for the additional reason that Plaintiffs did not plausibly allege that Google received such data. *See* A35 n.13 (the Court "cannot credit Plaintiffs' argument that Google intercepted communications containing birthdate and gender information"). Plaintiffs allege only that Viacom may have embedded its own internal "rugrats" codes, representing the age and gender of users, in URLs for Viacom webpages, and that these codes (not what they represent) were included in GET requests that users' browsers sent to Google. A82-83, 94. Plaintiffs do not allege that Google knew about the internal Viacom codes, much less

If Google obtained any such data, it did so through ordinary GET requests coming from Plaintiffs' browsers—not from the cookies. Indeed, Plaintiffs admit that Google would receive this data regardless of whether a cookie was placed on Plaintiffs' browsers. Pls.' Opp. at 43 ("Google would have received the inputted information, including the URL, regardless of the setting of third-party cookies."); *id.* at 34 (even without Google's cookie, "Google would still receive URLs in the form of GET requests"); A63-66, 68-69, 79-80, 94. Because this information was not intercepted by means of the cookies (the only alleged "device" that Google used), it cannot support a Wiretap Act claim. That is true regardless of whether URLs qualify as "contents," an issue addressed in Plaintiffs' and Viacom's brief,[7] but which this Court does not need to re-

---

that Google understood them. Nor do Plaintiffs allege any facts to show that Google's receipt of "rugrats" codes had anything to do with the DoubleClick ID cookie, rather than the routine back and forth between browsers and servers that occurs wholly independent of the presence or absence of cookies. *See* A63-66, 68-60, 79, 80, 94, 112-14, 116-17, 128-29.

[7] Plaintiffs' brief selectively quotes the oral argument transcript from *In re Google Cookie Placement Consumer Privacy Litigation*, No. 13-4300 (3d Cir.). *See* POB at 30-31. While Google's counsel explained that under certain circumstances (not present in the record of that case) URLs may amount to "contents" under the Wiretap Act, that is inappo-

solve in order to affirm the dismissal of the Wiretap Act claim against Google.

2. Google Was a Party to the Communication and Viacom Consented to Any Alleged Interception

Second, there can be no Wiretap Act violation because Google was a party to the communications that it allegedly intercepted and Viacom consented to any such interception. The Wiretap Act allows interception by anyone who 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); *accord Caro v. Weintraub*, 618 F.3d 94, 100 (2d Cir. 2010). Courts have long recognized that third-party Internet advertising services like Google are either parties to GET request communications or have consent to receive them. *See, e.g.*, *DoubleClick*, 154 F. Supp. 2d at 510-11, 514; *Chance v. Ave. A, Inc.*, 165 F. Supp. 2d 1153, 1162 (W.D. Wash. 2001); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 713 (N.D. Cal. 2011). That is the case here, as the District Court properly concluded. *See* A31.

---

site here, and the Court need not reach this issue for the reasons explained above.

Party to the Communication. Google was a party to Plaintiffs' alleged communications, including the URLs and cookie values, because the exchange of information was in the form of GET requests sent directly from Plaintiffs' browsers to Google. A63-66, 68-69, 79, 80, 94, 112-13, 116-17, 128-29. Indeed, Plaintiffs *concede* that they deliberately sent these GET requests to Google. POB at 35 ("The Plaintiffs and American Internet users in general, do not just accidentally send GET requests with random URLs. Internet communications consist *of deliberate acts*.") (emphasis added); *id.* (such communications "involve a conscious choice by the user to request such information.").[8] Under the Wiretap Act, Google does not "intercept" communications that are deliberately

[8] To be sure, Plaintiffs also make conclusory, implausible allegations that Google cookies receive information directly from *Viacom's* cookies and that Viacom "provided Google with access to the profile and other information contained within Viacom's first party cookies." *See, e.g.*, A127-28. Plaintiffs do not explain how communications can somehow be transmitted through cookies, which are just alphanumeric text files. *See* A114, 117-18. Nor do Plaintiffs allege facts to explain how—contrary to the ordinary operation of cookies on the Internet—cookies set by Viacom on the Viacom domain can somehow be accessed and read by Google. *See In re Hulu Privacy Litig.*, No. 11-cv-3764, 2014 U.S. Dist. LEXIS 83661, at *15 (N.D. Cal. June 17, 2014) ("The only servers that can access a particular cookie are those associated with the domain that wrote the cookie.").

sent to it in this way. *See, e.g.*, *Goode v. Goode*, No. 99-432-SLR, 2000 U.S. Dist. LEXIS 3124, at *8 (D. Del. Mar. 14, 2000).

Consent. Plaintiffs try to get around this result by arguing that they did not consent to the alleged interception.[9] This argument fails. As an initial matter, Plaintiffs ignore that the "party to the communication" defense is separate from a consent defense (18 U.S.C. § 2511(2)(d)). Because Google was a party to the alleged communications as explained above, separate consent is not necessary to defeat Plaintiffs' claim. Moreover, to the extent consent is relevant, the District Court correctly ruled that Viacom consented to any communications allegedly intercepted by Google. A31. The Viacom websites that Plaintiffs allegedly visited were also parties to the communications with Plaintiffs' browsers, and Viacom indisputably authorized Google's access to those communications. A68-69, 78, 82, 92.

[9] To the extent Plaintiffs suggest that "consent" is an affirmative defense that cannot be raised on a motion to dismiss, that is clearly wrong. A complaint may be dismissed where an affirmative defense "appears on its face." *Victaulic Co. v. Tieman*, 499 F.3d 227, 234-35 (3d Cir. 2007). That Plaintiffs consented to any acquisition of the communications at issue by Google is apparent from the face of their Complaint.

Plaintiffs argue that because Plaintiffs are minors, they cannot consent, and Google thus cannot invoke this defense. But the District Court properly rejected this argument, recognizing that because the Wiretap Act is a "one-party consent" statute, only Viacom's consent is needed. Whether Plaintiffs consented (or are legally capable or consent) is irrelevant under the Wiretap Act. A31 (citing 18 U.S.C. § 2511(d)(2) [sic]). Indeed, Plaintiffs' interpretation would produce absurd results. If a minor's age somehow invalidated the Wiretap Act's one-party consent exception, every person or company that ever received a call, voicemail, email, or text from a minor would violate the Wiretap Act. That result would have catastrophic effects for everyday communications.

None of the cases Plaintiffs cite are to the contrary. Plaintiffs cite the same inapposite Supreme Court cases that they cited below. As the District Court explained, this "sextet of Supreme Court decisions … have no application to these facts—they are a mix of death penalty, criminal sentencing, and abortion cases that have no bearing on the Court's task in this case." A33. Plaintiffs also cite *L.C. v. Central Pa. Youth Ballet*, No. 1:09-cv-2076, 2010 U.S. Dist. LEXIS 66060 (M.D. Pa. July 2, 2010), but that case denied the defendant's motion to dismiss

because the crime-tort exception applied, not because the case involved a minor. And *Bishop v. State*, 241 Ga. App. 517, 522 (1999) involves Georgia's Wiretap Act, which (unlike the federal Wiretap Act) contains language specifying under what circumstances a child may consent.

Crime-Fraud Exception. To try to save their claim, Plaintiffs seek to invoke an exception to the consent and "party to the communication defense," which permits defendants to be held liable if they intercept communications "for the purpose of committing any criminal or tortious act." 18 U.S.C. § 2511(2)(d). Plaintiffs argue that they satisfied this exception because Google's alleged interceptions also constitute an intrusion and a violation of various federal laws. Plaintiffs are mistaken.

As an initial matter, Plaintiffs' allegations are mere "formulaic recitation[s]" without support, and are properly ignored. *Iqbal*, 556 U.S. at 678. In any event, Plaintiffs' argument is based on a fundamental misunderstanding about the crime-tort exception. This exception only applies "if [the interception was] made 'with an *unlawful motive*,' such as 'blackmailing the other party, threatening him, or publicly embarrassing him.'" *Caro*, 618 F.3d at 99 (emphasis added). Plaintiffs thus would need to allege that Google had "as [its] objective a tortious or

criminal result," *id.* at 100, and that the tortious or criminal act was "independent of the intentional act" of interception. *Id.*; *Berk v. J.P. Morgan Chase Bank, N.A.*, No. 11-2715, 2011 U.S. Dist. LEXIS 143510, at *8 (E.D. Pa. Dec. 13, 2011); *see also 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.").

The District Court correctly held that Plaintiffs cannot invoke this exception because this case is "not [about] an illegal purpose." *See* A32; A8 (Google's purpose is "'to sell targeted advertising'"); *see also DoubleClick*, 154 F. Supp. 2d at 518 (rejecting application of criminal purpose exception because use of DoubleClick ID cookie was to "execut[e] a highly-publicized market-financed business model in pursuit of commercial gain"). Indeed, Plaintiffs concede that Google's purpose was to provide a valued service to commercial websites, and not to perpetuate a tort or crime. A59 ("[U]nique and specific electronic identifying information and content about each of these children was accessed, stored, and utilized *for commercial purposes*." (emphasis added)).

On appeal, Plaintiffs do not challenge the District Court's finding that Plaintiffs did not allege an unlawful purpose. Plaintiffs instead suggest that they do not need to allege an unlawful purpose independent of the act of interception to invoke this exception; they claim an intentional and unwanted interception is enough. Plaintiffs are wrong. Under this circular theory, anyone who receives a communication intending to use it for a purpose not subjectively desired by the sender would violate the Wiretap Act. That is not the law. *See Caro*, 618 F.3d at 98-99 ("the defendant must have the intent to use the illicit recording to commit a tort o[r] crime beyond the act of recording itself.").[10]

3. Plaintiffs' Barebones Allegation that Google Tracked Plaintiffs' Communications with Other Websites Does Not State a Wiretap Act Claim

Plaintiffs argue that "the District Court failed to address directly Plaintiffs' Wiretap claim relating to interceptions of their communica-

[10] *Deteresa v. American Broadcasting Companies* is not to the contrary: the court *granted summary judgment to the defendant* after the plaintiff failed to produce evidence of an illegal purpose. 121 F.3d 460, 467 n.4 (9th Cir. 1997). Moreover, the Ninth Circuit subsequently confirmed that "[w]here the purpose is not illegal or tortious, but the means are, the victims must seek redress elsewhere." *Sussman v. Am. Broad. Cos.*, 186 F.3d 1200, 1202-13 (9th Cir. 1999).

tions with non-Viacom websites." POB at 41. That is simply untrue. The District Court concluded that Plaintiffs' allegations about "'other websites on which Google places advertisements'" are "conclusory" and "made with no factual support." A31 n.12. The Court was exactly right: Plaintiffs' allegations are contained in a single paragraph (A97) and do not assert, among other things, what websites Plaintiffs visited, what information Google allegedly collected, whether these websites consented to Google's alleged tracking, or even what type of cookie was used. These "conclusory" allegations were properly disregarded. *Twombly*, 550 U.S. at 555.

B. PLAINTIFFS CANNOT STATE A CIPA CLAIM

As the District Court recognized, the elements of a CIPA claim are essentially identical to those of a federal Wiretap Act claim. A39. The CIPA claim against Google thus fails for the same reasons set out above. Plaintiffs' efforts to escape this result do not work.[11]

[11] 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.

First, Google is a party to the communications at issue in this case because Plaintiffs intentionally sent these communications as GET requests directly to Google. *See supra* pp. 6-7. *See Membrila v. Receivables Performance Mgmt., LLC*, No. 09-cv-2790-IEG, 2010 U.S. Dist. LEXIS 33565, at *4 (S.D. Cal. Apr. 6, 2010); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d at 713. Plaintiffs argue that this does not matter because CIPA is an "all-party consent statute" and they did not give their consent. POB at 42. But Plaintiffs mischaracterize the law. The provision of CIPA at issue here (section 631) only applies to wiretapping "by a third party"—not a "participant" in the communication. *See Warden v. Kahn*, 160 Cal. Rptr. 471, 475 (Cal. Ct. App. 1979); *Powell v. Union Pac. R.R. Co.*, 864 F. Supp. 2d 949, 955 (E.D. Cal. 2012).

Second, Plaintiffs fail to allege the interception of the contents or meaning of a protected communication. "Contents or meaning" under California law means the same as "contents" under federal law. A39. As explained above (*supra* pp. 25-26), the only relevant communications here are cookie values, which are not contents. Cal. Penal Code § 631(a); *Cookie Litig.*, 988 F. Supp. 2d at 445 (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). Because Google did not intercept the contents or meaning of Plaintiffs' communications, the District Court properly dismissed Plaintiffs' CIPA claim.

C. PLAINTIFFS CANNOT STATE AN SCA CLAIM

The District Court also correctly held that Plaintiffs do not state a claim under the Stored Communications Act ("SCA"). The SCA requires Plaintiffs to allege facts showing Google "intentionally accesse[d] without authorization a facility through which an electronic communication service is provided … and thereby obtain[ed] … a wire or electronic communication while it is in electronic storage in such system." 18 U.S.C. § 2701(a). Plaintiffs' SCA allegations fail for three independent reasons.

1. Plaintiffs Cannot Allege That The Cookies Enabled Google to "Obtain" Their Communications

The SCA is violated only where the defendant "obtained" a communication as a result of accessing a facility without authorization. Here, however, Google's allegedly unauthorized placement of cookies

did not cause Google to "obtain" any of Plaintiffs' communications. As explained above, the communications at issue (including URLs) were sent to Google via Plaintiffs' browsers' GET requests regardless of whether any cookies were present. *Supra* pp. 26-27. There thus is no causal relationship between Google's supposedly wrongful access and its obtaining the communications at issue. That defeats any SCA claim.

2. Plaintiffs' Personal Devices and Browsers Are Not the "Facilities" of an "Electronic Communication Service" Protected by the SCA

The SCA claim also fails because Plaintiffs' browsers are not "electronic communication service" (ECS) providers, and browser files that contain cookies are not "facilities" protected by the SCA. "An individual's personal [computer or mobile device] does not *provide* an electronic communication service just because the device *enables* use of electronic communication services …." *Garcia v. City of Laredo*, 702 F.3d 788, 793 (5th Cir. 2012). Instead, "[t]he statute envisions a *provider* (the ISP or other network service provider) and a *user* (the individual with an account with the provider), with the *user's communications in the possession of the provider*." *Id.* (citation omitted); *see also United States v.*

Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003) (the SCA "does not appear to apply to … hacking into [a personal] computer").

That is confirmed by the structure of the statute. The browser software applications on Plaintiffs' computers and mobile devices cannot be ECS providers because that software is not capable of performing the many functions required of ECS providers by the SCA. For example, an ECS provider must be capable of granting and revoking authorization to users to use the ECS. 18 U.S.C. § 2510(13)(B). ECS providers must also be capable of having "officers, employees, and agents, landlords, [and] custodians," 18 U.S.C. § 2511(2)(a)(ii), and of being subject to court orders and judgments and following directions from the government, *id.* Browsers cannot do any of that.

Just as Plaintiffs' browsers cannot be an ECS provider, the District Court correctly concluded that a "personal comput[ing device] is not 'a facility through which an electronic communication service is provided,'" as required under the SCA. A37-38 (quoting *Morgan v. Preston*, No. 13-cv-0403, 2013 WL 5963563, at *7 (M.D. Tenn. Nov. 7, 2013)). That is because the "the relevant 'facilities' that the SCA is designed to protect are not computers that *enable* the use of an electronic communi-

cation service, but instead are facilities that are *operated by* electronic communication service providers and used to store and maintain electronic storage." *Garcia*, 702 F.3d at 792 (quoting *Freedom Banc Mortg. Servs., Inc. v. O'Harra*, No. 11-1073, 2012 WL 3862209, at *9 (S.D. Ohio Sept. 5, 2012) (emphasis in original)); *see also Cousineau v. Microsoft Corp.*, 6 F. Supp. 3d 1167, 1175 (W.D. Wash. 2014) (smartphone is not a facility); *Council on Am.-Islamic Relations Action Network, Inc. v. Gaubatz*, 793 F. Supp. 2d 311, 334-35 (D.D.C. 2011) (no SCA claim if access was only to plaintiffs' computers). Simply put, as the Fifth Circuit recently held, a "home computer of an end user is not protected by the SCA." *Garcia*, 702 F.3d at 793 (quoting Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208, 1215 (2004)). Any other "construction would render other parts of the statute illogical." *In re iPhone Application Litig.* ("*iPhone II*"), 844 F. Supp. 2d 1040, 1058 (N.D. Cal. 2012).[12]

[12] For example, the SCA authorizes ECS providers to grant access to a "facility" (18 U.S.C. § 2701(c)(1)), and holding that a user's computer is a "facility" thus would mean that ECS providers could grant third parties access to users' home computers. *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1270-71 (N.D. Cal. 2001). "Such a result would be illogical[.]" A38.

Plaintiffs have no meaningful response to this "'overwhelming body of law.'" A37 (quoting *Morgan*, 2013 WL 5963563, at *5). Many of the cases they cite (POB at 45) are inapplicable because they do not discuss what constitutes an SCA "facility" (*Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 902 (9th Cir. 2008)), or because they involve the facilities of a *business* that was allegedly an electronic communications service provider (*Becker v. Toca*, C.A. No. 07-7202, 2008 U.S. Dist. LEXIS 89123, at *12 (E.D. La. Sept. 24, 2008)). The rest are outdated outliers that have been rejected by subsequent courts because they "provide little analysis on this point of law, instead assuming the plaintiff's position to be true due to lack of argument and then ultimately ruling on other grounds." *iPhone II*, 844 F. Supp. 2d at 1057-58. This Court should affirm the District Court's ruling on this point—and avoid creating a circuit split—by holding that Plaintiffs' personal devices are not protected by the SCA.

3. Plaintiffs Cannot Allege a Communication Accessed While in "Electronic Storage"

Finally, Plaintiffs cannot state an SCA claim because they identify no "communication" that was in "storage" by an ECS provider when ac-

cessed by Google. "'Electronic storage' as defined encompasses only the information that has been stored by an electronic communication service provider" and only "if such information is stored temporarily pending delivery." *Garcia*, 702 F.3d at 793; 18 U.S.C. § 2510(17)(A) ("'electronic storage' means … any *temporary*, *intermediate* storage of a wire or electronic communication *incidental to the electronic transmission thereof*" (emphasis added)); *see also, e.g.*, *DoubleClick*, 154 F. Supp. 2d at 511-12 ("[a]ny temporary, intermediate storage … describes an e-mail message that is being *held by a third-party Internet service provider*").

The SCA's references to "intermediate" storage "incidental to the electronic transmission thereof" reflect the SCA's purpose to "protect[] electronic communications stored 'for a limited time' in the 'middle' of a transmission, *i.e.* when an electronic communication service temporarily stores a communication while waiting to deliver it." *DoubleClick*, 154 F. Supp. 2d at 512; *see also Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001) (the SCA "covers a message that is stored in intermediate storage temporarily, after the message is sent by the sender, but *before* it is retrieved by the intended recipient" (empha-

sis added)), *aff'd in part, vacated in part on other grounds*, 352 F.3d 107, 114 (3d Cir. 2003) (communications in "post-transmission storage" are "not in temporary, intermediate storage").

Plaintiffs here cannot state an SCA claim based on Google's receipt of GET requests because these were not communications in storage "waiting to [be] deliver[ed]" to a third party when Google received them.[13] To the contrary, these GET requests sent to Google were created specifically for Google and intentionally sent directly to Google by Plaintiffs' browsers when viewing websites with Google ads. *See* Pls.' Opp. at 34 ("Google … receive[d] URLs in the form of GET requests"); *id.* at 43 ("'Google would have received the inputted information, including the URL, regardless of the setting of third-party cookies'"); POB at 35 ("The Plaintiffs and American Internet users in general, do not just accidentally send GET requests with random URLs. Internet communications consist of deliberate acts."); A63-66, 68-69, 79-80, 94. They were

[13] Tellingly, Plaintiffs allege elsewhere in the Complaint that these communications were not in storage but "in transit" and received by Google "contemporaneously" with transmission. A65, 69.

thus not in storage "incidental" to being transmitted to anyone but Google.

Nor can Plaintiffs state an SCA claim based on Google's receipt of the cookies it placed on Plaintiffs' browsers because, as Plaintiffs allege, these cookies were "persistent" (not temporary) and designed to stay on a person's computing device "for years." A67-68. Regardless of whether a copy of the cookies was *also* temporarily stored in random access memory (RAM), their alleged permanent storage on Plaintiffs' hard drives means that they were not being "stored temporarily pending delivery [to another party] or for purposes of backup protection," as required by the SCA. *Garcia*, 702 F.3d at 793.

Plaintiffs' SCA claim fails for each of these reasons.

D. PLAINTIFFS CANNOT STATE A VPPA CLAIM

To state a claim under the VPPA, Plaintiffs must allege (1) a Video Tape Service Provider ("VTSP"), (2) "knowingly disclose[d], to any person," (3) personally identifiable information ("PII"), (4) "concerning any consumer of such provider," unless an exception applies. 18 U.S.C. § 2710(b)(1). The District Court correctly dismissed this claim because

Google is not a VTSP and because Google did not disclose Plaintiffs' PII to any third party.

1. 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 do not even try to allege that Google meets this definition. A91 (only attempting to plead facts establishing that Viacom satisfies definition); A18 ("the MCC does not allege [that] Google is a VTSP"). Instead, relying entirely on *Dirkes v. Borough of Runnemede*, 936 F. Supp. 235 (D.N.J. 1996), Plaintiffs argue that *any person* who possesses PII can be sued under the VPPA, even if they are not VTSPs.

Dirkes was wrongly decided, as the District Court and a "great majority of courts to address the issue" have explained. A16. *First*, *Dirkes* ignores the plain statutory language, which only authorizes a disclosure claim against a VTSP. *See* 18 U.S.C. § 2710(b)(1) ("A video tape service provider who knowingly discloses … shall be liable to the aggrieved person …"). *Second*, it would render Congress's detailed definition of a VTSP (*id.* § 2710(a)(4)) superfluous. *See Daniel v. Cantrell*,

375 F.3d 377, 383 (6th Cir. 2004) (rejecting *Dirkes* on this basis). *Third*, such an expansive prohibition against disclosure would act as a prior restraint of speech. "The well-established doctrine of constitutional avoidance therefore counsels against reading the [VPPA] so broadly." *ACLU v. Holder*, 652 F. Supp. 2d 654, 669 (E.D. Va. 2009).

Noting that § 2710(c)(1) provides that "[a]ny person aggrieved by any act of a person in violation of this section may bring a civil action," 18 U.S.C. § 2710(c)(1), Plaintiffs argue that any "person" may be a defendant. But this ignores the words "in violation of this section," which make clear that only a person who actually violates the VPPA is subject to suit. As the District Court recognized, under § 2710(b)(1), the only person who can violate the VPPA's disclosure provision is a VTSP. "It is thus apparent on the face of the VPPA that an 'aggrieved' person's claim must be against a 'video tape service provider.'" A16; *Daniel*, 375 F.3d at 381-82; *Hulu*, 2014 WL 1724344, at *7. Because Plaintiffs do not allege that Google is a VTSP, their claim fails as a matter of law.

2. Google Did Not Disclose Plaintiffs' PII

Even if Google were a VTSP, this claim would still have to be dismissed because Plaintiffs do not allege that Google "disclose[d]" Plain-

tiffs' information to a third party. 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). Indeed, as Plaintiffs admit, they only allege that "Viacom knowingly *disclosed*, and Google knowingly *obtained*" PII—not that Google disclosed PII. POB at 8 (emphasis added); *see also* POB at 27-28; A92. Without an alleged disclosure of PII there can be no VPPA claim. *See, e.g.*, *Rodriguez v. Sony Computer Entm't Am. LLC*, No. c-11-4084, 2012 U.S. Dist. LEXIS 55959, at *3-4 (N.D. Cal. Apr. 20, 2012) (dismissing VPPA claim 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").[14]

[14] As Plaintiffs' VPPA claim against Google fails for the foregoing reasons, the Court need not consider whether information allegedly disclosed to Google (*see* A92) constitutes "personally identifiable information" under the VPPA. *See* 18 U.S.C. § 2710(a)(3) (defining term as "information which identifies a person as having requested or obtained specific video materials from" a VTSP). To the extent the Court considers the issue relevant, for the reasons set forth in Viacom's answering brief and the lower court's opinion (*see* A18-30), such information does not constitute "personally identifiable information."

E. PLAINTIFFS CANNOT STATE A NEW JERSEY CROA CLAIM

The District Court also properly dismissed Plaintiffs' New Jersey CROA claim. "The CROA is an anti-computer-hacking statute." A40. CROA claims are "similar" to Computer Fraud and Abuse Act ("CFAA") claims and "mirror" claims under § 502 of the California Penal Code (the "CCL"). *Mu Sigma, Inc. v. Affine, Inc.*, No. 12-1323, 2013 U.S. Dist. LEXIS 99538, at *30 (D.N.J. July 17, 2013); *Joseph Oat Holdings, Inc. v. RCM Digesters, Inc.*, 409 F. App'x 498, 504 (3d Cir. 2010).[15] The CROA has never been applied to ordinary Internet activity of the type

[15] 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) (explaining that courts 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.*, No. C-10-02389, 2011 U.S. Dist. LEXIS 147345, at *14 & n.8 (N.D. Cal. Nov. 22, 2011), *aff'd in part, rev'd in part, remanded by Facebook Privacy Litig. v. Facebook, Inc.*, 572 F. App'x 494 (9th Cir. 2014) (CCL not aimed at abuse of a "standard web browser function"). The CROA should be interpreted through the lens of that same policy objective. *See* A40 (describing the CROA as an "anti-hacking statute").

Plaintiffs challenge here, and claims challenging such conduct have been repeatedly rejected under both the CCL and CFAA. *See, e.g.*, *In re iPhone Application Litig.*, No. 11-MD-02250, 2011 U.S. Dist. LEXIS 106865, at *33-41 (N.D. Cal. Sept. 20, 2011); *In re Google Android Consumer Privacy Litig.*, No. 11-MD-02264, 2013 U.S. Dist. LEXIS 42724, at *21-24, *33-37 (N.D. Cal. Mar. 26, 2013); *see also Cookie Litig.*, 988 F. Supp. 2d at 447-50. Thus, Plaintiffs are "seek[ing] to fit square pegs into round holes." A53.

To state a claim under the CROA, Plaintiffs must allege that Google (1) "damaged [Plaintiffs] in business or property" by (2) engaging in enumerated conduct. N.J. Rev. Stat. § 2A:38A-3 (2013). Plaintiffs cannot satisfy either element.

1. Google Did Not Damage Business or Property

Plaintiffs did not plausibly allege that Google "damaged [Plaintiffs] in business or property." *Id.* Plaintiffs cite a single paragraph in their SAC that they claim alleges an unjust enrichment theory of damages "in a quasi-contractual sense." POB at 47; A155.

As an initial matter, these allegations are unsupported and too conclusory to be considered on a motion to dismiss. *Twombly*, 550 U.S.

at 555 (a complaint "requires more than labels and conclusions"). But even if credited, Plaintiffs' effort to rely on unjust enrichment to support their CROA claim fails because "[t]his is not a quasi-contract case." A43. While Plaintiffs suggest that they entered a contractual or quasi-contractual relationship with Viacom through their use of Viacom's website (POB at 48-49), those allegations have no bearing on Google.

Even assuming that Plaintiffs entered into a "quasi-contract" relationship with Google, Plaintiffs have not alleged facts indicating unjust enrichment. To allege unjust enrichment, a party must demonstrate "'that it expected remuneration from the defendant at the time it performed or conferred a benefit on defendant and that the failure of remuneration enriched defendant beyond its contractual right.'" POB at 47-48 (quoting A43 & citing *VRG Corp. v. GKN Realty Corp.*, 641 A.2d 519, 554 (N.J. 1994)). Plaintiffs did not allege any facts that show they could reasonably expect any remuneration from Google. "[J]ust because Defendants could monetize Plaintiffs' Internet usage did not necessarily mean that Plaintiffs could do the same." A53.

Moreover, even if Plaintiffs could somehow monetize their Internet usage, Plaintiffs did not allege any facts showing that Google's

"conduct prohibited them from still doing so." A54; *see also Cookie Litig.*, 988 F. Supp. 2d at 448 ("[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 plaintiffs' computers, systems or data that could require economic remedy."); *Low v. LinkedIn Corp.*, No. 11-cv-01468, 2011 U.S. Dist. LEXIS 130840, at *10-15 (N.D. Cal. Nov. 11, 2011) (general allegations that consumer information is valuable and that plaintiffs were not compensated for use of their information are insufficient to show injury); *see also supra* pp. 18-20.

Finally, Plaintiffs cite no authority indicating that the claimed "unjust enrichment" to Google could possibly constitute damage to their business or property to satisfy the CROA. Cases that have found damage to "business or property" under the CROA involve actual economic detriment to plaintiffs, not merely a claimed benefit to defendants. *See, e.g.*, *P.C. of Yonkers, Inc. v. Celebrations! The Party & Seasonal Superstore, LLC*, C.A. No. 04-4554, 2007 U.S. Dist. LEXIS 15216, at *27 (D.N.J. Mar 2, 2007) (plaintiffs suffered "great financial detriment" because defendants allegedly used data stolen from plaintiffs to unfairly

compete against them); *Fairway Dodge, Inc. v. Decker Dodge, Inc.*, No. A-1736-03T2, 2006 N.J. Super. Unpub. LEXIS 1360, at *28 (App. Div. June 12, 2006) (defendants' conduct "impaired [plaintiff's] opportunity to sell vehicles, parts, and services and … such impairment resulted in lost revenue."), *aff'd*, 191 N.J. 460 (2007).

Because "Plaintiffs have … failed to identify any property or business damage, as is required" (A54), their claim fails.

2. Plaintiffs Do Not Meet the Remaining CROA Requirements

Plaintiffs' CROA claim fails for the additional reasons that (1) Plaintiffs allege no facts that Google engaged in any conduct prohibited by the statute, and (2) Plaintiffs allege no facts that Google purposefully or knowingly harmed them.

a. Plaintiffs Do Not Allege Prohibited Conduct

Plaintiffs cannot and do not allege facts sufficient to show that Google engaged in any of the specific conduct prohibited by the CROA.

CROA Subsections 3(a)-(b). Plaintiffs do not state claims under subsections 3(a)-(b) because they do not allege that Google caused any alteration, damage, taking, or destruction of any data or computer. Ra-

ther, Google merely communicated with Plaintiffs' browsers as those browsers were designed to communicate. A112-14, 116-17. Nor did Google engage in an unauthorized taking. Any information it received was *voluntarily sent to it* by Plaintiffs' browsers via a GET request—a routine and necessary part of Internet browsing. Plaintiffs admit that the only additional information Google obtained by placing cookies on Plaintiffs' browsers was information that it already knew and that it had permission to access: its cookie values. A117-18. Google would receive all the other information whether or not a cookie was present on their browsers. *See* Pls.' Opp. at 34 ("Google would still receive URLs in the form of GET requests"); *id.* at 43 (acknowledging that "'Google would have received the inputted information, including the URL, regardless of the setting of third-party cookies'") (quoting *Cookie Litig.*, 988 F. Supp. 2d at 444-45).

Even under Plaintiffs' unsupported theory that Google received information in some way directly from Viacom, Plaintiffs admit that Viacom *shared* information with Google or *provided Google with access* to it. *See supra* p. 30. They do not allege that Google affirmatively *took* anything without authorization. The CROA requires "proof of some activi-

ty vis-a-vis the information other than simply gaining access to it." *P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC*, 428 F.3d 504, 509 (3d Cir. 2005); *PNC Mortg. v. Superior Mortg. Corp.*, No. 09-5084, 2012 U.S. Dist. LEXIS 25238, at *14 (D.N.J. Feb. 27, 2012) (dismissing CROA claim where "there are no facts that show that any data or information was taken ….").

CROA Subsection 3(c). Plaintiffs cannot state a subsection 3(c) claim because they cannot show that Google accessed a computer without authorization, which requires conduct akin to *hacking*. *See P.C. Yonkers*, F.3d 428 at 509; A53 ("the CROA targets computer hacking"). 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]; *Joseph Oat Hold-*

[16] While *Chrisman* interpreted the CCL, the CROA defines the term "access" similarly and should therefore be interpreted similarly. *Compare* N.J. Rev. Stat. § 2A:38A-1(a) (2013) ("'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. Penal Code § 502(b)(1) ("'Access' means to gain entry to, instruct, or communicate with the logical, arithmetical, or memory

ings, 409 F. App'x. at 503, 504, 506 (same). The SAC admits that any access Google had to Plaintiffs' information was accomplished only through an authorized exchange of information with Plaintiffs' browsers. A112-13, 116-18; *see also supra* pp. 6-7. And as noted, the only information Google obtained by placing cookies on Plaintiffs' browsers were the values of Google's own cookies, which it already knew because it created those values. A117-18.

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

CROA Subsection 3(e). Plaintiffs' subsection (e) claim fails because, as discussed above, they do not plead facts that Google *hacked* their computers. Plaintiffs also offer no facts to suggest that Google acted "recklessly" in any way; indeed Plaintiffs' own allegations demonstrate that Google engaged in routine Internet communications and not in any conduct that can be deemed reckless.

---

function resources of a computer, computer system, or computer network.").

b. Google Did Not Purposefully or Knowingly Harm Plaintiffs

"[E]ach subsection [of the CROA] requires that the conduct by [the defendant] be purposeful or knowing." *Fairway Dodge, LLC v. Decker Dodge, Inc.*, 191 N.J. 460, 469 (2007) (quotations omitted); *Spencer Sav. Bank SLA v. McGrover*, No. A-1899-13T3, 2015 N.J. Super. Unpub. LEXIS 459, at *19 (N.J. App. Div. Mar. 5, 2015) (CROA requires "a showing of 'purposeful or knowing' conduct"). Accordingly, consistent with similar requirements under the CFAA,[17] 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. Plaintiffs cannot satisfy this element here because their allegations confirm that Google's purpose in placing cookies on their computers was to deliver more relevant ads, not to in-

[17] *Kalow & Springnut, LLP v. Commence Corp.*, No. 07-3442, 2008 U.S. Dist. LEXIS 48036, at *9 (D.N.J. June 23, 2008) (dismissing CFAA claim where plaintiff failed to allege "that [defendant] intended to cause *harm*, i.e. actual intent"); *Oracle Corp. v. SAP AG*, 734 F. Supp. 2d 956, 964 (N.D. Cal. 2010) ("plaintiffs must allege and prove that [the defendant] specifically 'intended' to 'cause damage'"); *Devon Energy Corp. v. Westacott*, No. 09-1689, 2011 U.S. Dist. LEXIS 30786, at *32-34 (S.D. Tex. Mar. 24, 2011) (collecting cases).

jure Plaintiffs' business or property. A115-16, 118; *see* A8-9 ("The information is used by Google … 'to sell targeted advertising'"); A32-33; *DoubleClick*, 154 F. Supp. 2d at 519.

F. PLAINTIFFS CANNOT STATE AN INTRUSION CLAIM

Finally, the District Court correctly held that Plaintiffs fail to state an intrusion claim. That ruling should be affirmed because Plaintiffs do not plausibly allege 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)).

1. Google Did Not Invade a Legally Private Matter

First, Plaintiffs do not allege facts showing that Google invaded a legally private matter.[18] As the District Court explained, "the SAC simply includes no allegation that Google can identify the individual Plaintiffs in this case, as opposed to identifying people generally, nor any allegation that Google has actually done so here." A52. Plaintiffs

[18] Contrary to Plaintiffs' claim that the District Court "found Plaintiffs' Complaint sufficient with respect" to this element, POB at 50, the Court in fact did not reach this issue. A42; A54-57.

premise their claim on the assertion that Google collects PII when users register accounts for certain Google services not at issue here (*e.g.*, Gmail, Google Plus), and "connects" this information to cookies. A80-82. Thus, "[a]ccording to Plaintiffs, in order for Google to connect the information that Viacom provides it with the identity of an individual Plaintiff, one of the Plaintiffs would need to have registered on one of Google's services." A52.

These allegations do not help Plaintiffs because *they do not and cannot allege that they are Google account holders*. A109-10 (only alleging that Plaintiff "has been a registered user of the website Nick.com"); A52 ("Plaintiffs have alleged no facts whatsoever that a Plaintiff ever registered with Google."). Indeed, because Plaintiffs are under 13 years old, Google prohibited them from registering for an account. A52.[19]

Plaintiffs try to fix this glaring defect on appeal by asserting in a footnote that Plaintiffs' *parents* had Google accounts. POB at 22 n.6.

[19] Plaintiffs' allegations are implausible for the additional reason that they are inconsistent with Google's privacy policy, a point Plaintiffs did not dispute while before the District Court. *See* SAC ¶ 85 ("'We will not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent'" (quoting privacy policy)).

But Plaintiffs "cannot amend [their] complaint on appeal by alleging new facts in [their] appellate brief." *Renovitch v. Kaufman*, 905 F.2d 1040, 1049 n.12 (2d Cir. 1990). And even if they could, this additional fact is irrelevant because Plaintiffs' parents are not parties in this case. Whether Google "tracked" Plaintiffs' parents is irrelevant. Because Plaintiffs do not allege an invasion of a legally private matter, their intrusion claim fails as a matter of law.[20]

2. The Alleged Intrusion Was Not Highly Offensive

Plaintiffs also fail to establish that the alleged intrusion was highly offensive to a reasonable person. As the District Court explained, "[s]urveying the classic intrusion … claims demonstrates that this tort supports allegations of *truly exceptional conduct*." A56 (citing cases & emphasis added). Unlike the egregious conduct alleged in those cases,

---

[20] While the *amicus curiae* brief filed by the Electronic Privacy Information Center ("EPIC") discusses a number of mechanisms with the potential for "tracking" individuals' activities online, such as "supercookies," "fingerprinting," and IPv6 addresses, none of those mechanisms is at issue here and there are no allegations in the record to support their use by Google or Viacom here. *See* Br. of *Amicus* Curiae Electronic Privacy Information Center (EPIC) in Support of Appellants, at 18-31. Thus, EPIC's allegations are irrelevant to Plaintiffs' intrusion claim.

Google's alleged receipt of information from Plaintiffs' browsers, and its use of cookies to display more relevant ads, "falls short of that kind of 'highly offensive' behavior." *See* A56.

Other courts have reached the same conclusion. *See Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1025-26 (N.D. Cal. 2012) (disclosure of browsing history not highly offensive); *iPhone II*, 844 F. Supp. 2d at 1063 (finding transfer of plaintiffs' geolocation information, personal data and unique device identifier number was not an egregious breach of social norms); *In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 987 (N.D. Cal. 2014) (finding alleged commingling and disclosure of PII is not highly offensive); *Yunker v. Pandora Media, Inc.*, No. 11-cv-03113, 2013 U.S. Dist. LEXIS 42691, at *44-45 (N.D. Cal. Mar. 26, 2013) (disclosing PII not highly offensive); *Cookie Litig.*, 988 F. Supp. 2d at 449-50 (neither "transfer of inputted information" nor "Google's subsequent association [of this data] to provide targeted advertising" constitutes a "sufficiently serious invasion of privacy").

Plaintiffs make no attempt to distinguish or dispute this overwhelming authority.[21] Instead, they raise a series of baseless arguments. *First*, Plaintiffs argue that Google's conduct is highly offensive because it supposedly violates the VPPA, the Wiretap Act, the Pen Register Act, the CFAA, and "corresponding computer crime statutes of all 50 states" in some unexplained way. POB at 59.[22] Because Plaintiffs do not even attempt to plead violations of the Pen Register Act, CFAA, and the "computer crime statutes of all 50 states," the Court must "disregard [these] 'naked assertions.'" *Santiago*, 629 F.3d at 131. Moreover, Plaintiffs' VPPA, Wiretap Act, and SCA allegations are not plausible for the reasons discussed above.

---

[21] Ignoring these numerous analogous cases where courts dismissed plaintiffs' intrusion claims, Plaintiffs argue that the determination of what is "highly offensive" is a question of fact that a jury, not a court, should decide. *See* POB at 51-52. The District Court correctly explained that "courts are … empowered to make that determination if it can be decided as a matter of law." A55 (citing *Boring v. Google*, 362 F. App'x 273, 279 (3d Cir. 2010)).

[22] Plaintiffs also suggest that Google somehow violated the New Jersey and U.S. Constitutions (POB at 58), even though their SAC does not allege this. Because Plaintiffs cannot amend the SAC through their appellate brief, this argument should be disregarded. *See Renovitch*, 905 F.2d at 1049 n.12.

In any event, merely alleging that conduct violates state or federal law is insufficient to show that it is highly offensive. *E.g.*, *Rush v. Portfolio Recovery Assocs.*, 977 F. Supp. 2d 414, 433-36 & n.23 (D.N.J. 2013) (plaintiffs failed to establish that the conduct was highly offensive even though it violated the Fair Debt Collection Practices Act); *Tamayo v. Am. Coradious Int'l, LLC*, No. 11-cv-6549, 2011 U.S. Dist. LEXIS 149124, at *11-12 (D.N.J. Dec. 28, 2011) (finding plaintiff's "bald assertions" that defendant violated Fair Debt Collection Practices Act not sufficient to show that conduct was highly offensive).

Second, Plaintiffs argue, again without explanation, that Google violated the "Terms of Use of Plaintiffs' Internet Service Providers and web browsers." POB at 58. But the provisions of the agreements that Plaintiffs reference govern the conduct of *consumers* using the services, not the conduct of *service providers* providing those services.[23] Those provisions have nothing whatsoever to do with an advertiser's use of cookies to provide benefits to web users. They certainly do not provide

[23] *See* A126-27 (referencing the privacy policies and terms of service of Internet service providers and web-browsers that prohibit "*users*" from engaging in "unlawful or unauthorized tracking of the communications of others…").

some yardstick against which that conduct could ever be judged highly or exceedingly offensive.[24]

Third, without any supporting fact allegations, Plaintiffs vaguely claim that Google's conduct was highly offensive because Google violated "the standards of the online advertising industry …." POB at 58. Plaintiffs do not explain this assertion other than to note that the online advertising industry supports compliance with Children's Online Privacy Protection Act ("COPPA"). *Id.* at 58-59. The Court must "disregard" these "'naked assertions.'" *Santiago*, 629 F.3d at 131. But even if these allegations were plausible, merely alleging that conduct violates such standards is insufficient to demonstrate that it is highly offensive. *Cf. Rush*, 977 F. Supp. 2d at 433-36 & n.23 (alleged violation of federal law not highly offensive); *In re Northwest Airlines Privacy Litig.*, 2004

[24] To the extent Plaintiffs are suggesting that Google somehow breached its own obligations under any of these agreements, that would still not be sufficient to establish that its conduct was highly offensive. *See In re Northwest Airlines Privacy Litig.*, No. 04-126, 2004 U.S. Dist. LEXIS 10580, at *13-18 (D. Minn. June 6, 2004) (disclosure of passenger information to government agency allegedly in violation of airline's privacy policy was not highly offensive).

U.S. Dist. LEXIS 10580, at *13-18 (alleged violation of privacy policy not highly offensive).

Fourth, Plaintiffs claim that Google "placed significantly more tracking technologies on children's websites than adult websites." POB at 57-58. But Plaintiffs' SAC only contains allegations about the relative number of cookies Viacom—not Google—placed on "children's sites." *See* A122. Moreover, the only website at issue in this case is Nick.com, so the number of times cookies were placed on other websites is irrelevant. And in any event, the fact that cookies are frequently used only confirms that their use is "routine commercial behavior" and not an "egregious breach … of social norms." *Low*, 900 F. Supp. 2d at 1025 (citation omitted).

Fifth, Plaintiffs cite the results of apparent consumer surveys. POB at 60-61. But these surveys reflect "sentiments that are not directly on point." A55. Many of the survey questions ask about completely irrelevant conduct. *See* A158-59 (asking about "tracking software"); A159 (asking about whether a hypothetical law "is a good idea"); *id.* (alleging that "[p]arents in the survey were more protective of children's privacy that non-parents"); *id.* (asking about "tracking your behavior across the

web"); A159-60 (asking "about the *government* or private companies collecting digital information from your computer or *phone*" (emphasis added)). None of the surveys purports to measure whether conduct is *highly offensive*. Instead, the surveys ask whether particular conduct is "wrong," A158; is "okay," A158-60; "should" require parental consent, A158-59; is "a good idea," A159; or causes "concern[]," A159-60. That is not the proper standard. As the District Court explained, "a large majority of voters may disapprove of a given politician's job performance, but that would not indicate that a reasonable person finds the politician's performance 'highly offensive.'" A56. Conduct must be "outrageous, rather than annoying or upsetting" to support an intrusion upon seclusion claim. *Rush*, 977 F. Supp. 2d at 435.

All of the survey questions are inapposite for the additional reason that they fail to consider the benefit of cookies. "[D]etermining whether an alleged invasion of privacy is substantial and highly offensive to the reasonable person necessitates the use of a balancing test." *Borse v. Piece Goods Shop, Inc.*, 963 F.2d 611, 627 (3d Cir. 1992). While consumers may dislike certain commercial conduct in the abstract, it is not highly offensive if it is socially useful. *Poltrock v. NJ Auto. Accounts*

Mgmt. Co., No. 3:08-1999, 2008 U.S. Dist. LEXIS 103351, at *20 (D.N.J. Dec. 17, 2008); *Vega v. United Recovery Sys., L.P.*, No. 11-5995, 2012 U.S. Dist. LEXIS 16801, at *15 (D.N.J. Feb. 9, 2012) (characterizing as "frivolous" allegation that debt collection call is "highly offensive"). Because the surveys alleged by Plaintiffs do not consider the social utility of cookies, they cannot possibly measure whether their use is "highly offensive."

Sixth, Plaintiffs argue that "Defendants obtained and disclosed personal information and Internet communications knowing the same could be traced or linked to identifiable young children," POB at 58, and that Google should have therefore accorded Plaintiffs unidentified special privacy protections because it knew they are children, *id.* at 56. But the SAC contains no facts that support this argument. As explained above, Plaintiffs' SAC only alleges that Viacom may have embedded internal "rugrats" codes reflecting children's ages and gender; Plaintiffs do not allege that Google knew about them or understood them. *See supra* note 6. Moreover, Plaintiffs' argument that Google knew it was collecting the PII of Plaintiffs is premised on the assumption that Plain-

tiffs have Google accounts—something that Plaintiffs do not and cannot allege, as explained above. *Supra* p. 58.

Because Google's alleged conduct "falls short of [the] kind of 'highly offensive' behavior" necessary to state an intrusion claim, the District Court's dismissal of this claim should be affirmed.

3. Google Lacked the Requisite Intent

Finally, the dismissal of Plaintiffs' intrusion claim should be affirmed because Google lacked the intent required to commit an unlawful intrusion.[25] "[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." *O'Donnell v. United States*, 891 F.2d 1079, 1083 (3d Cir. 1989)[26]; *Jevic v. Coca Cola Bottling*

[25] Here again Plaintiffs incorrectly claim that the District Court "found Plaintiffs' Complaint sufficient with respect" to this element (POB at 50), when in fact the Court did not reach this issue. A40-42; A54-57.

[26] While *O'Donnell* applies Pennsylvania law, both Pennsylvania and New Jersey courts have adopted the tort of intrusion as set forth in § 652B of the Restatement (Second) of Torts. *See O'Donnell*, 891 F.2d at 1082-83; *Burger v. Blair Med. Assocs.*, 964 A.2d 374, 379 (Pa. 2009); *Jevic*, 1990 U.S. Dist. LEXIS 8821, at *23-24; *G.D. v. Kenny*, 15 A.3d 300, 309 (N.J. 2011). As a result, "Pennsylvania common law [on the

Co., No. 89-4431, 1990 U.S. Dist. LEXIS 8821, at *23-24 (D.N.J. June 6, 1990) (following *O'Donnell*); *accord Dubbs v. Head Start, Inc.*, 336 F.3d 1194, 1221 (10th Cir. 2003).

Plaintiffs do not allege any facts indicating that 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; *see also* A32 ("[t]he instant lawsuit is … not [about] an illegal purpose"). Even Plaintiffs concede that Google acted "for commercial purposes." A108; A8-9 ("The information is used by Google … 'to sell targeted advertising'"); A32-33 (noting the absence of any facts indicating wrongful intent).

---

tort of intrusion] is virtually identical to New Jersey common law." *Rush*, 977 F. Supp. 2d at 433 n.23.

CONCLUSION

For these reasons, this Court should affirm the District Court's order dismissing Plaintiffs' claims against Google with prejudice.

Dated: June 15, 2015

WILSON SONSINI GOODRICH & ROSATI
Professional Corporation

By: /s/ Colleen Bal

Colleen Bal (CA Bar No. 167637)
Michael H. Rubin (CA Bar No. 214636)
One Market St., Spear Tower, Ste. 3300
San Francisco, California 94105
Telephone: (415) 947-2000

Attorneys for Defendant-Appellee
Google Inc.

CERTIFICATE OF COMPLIANCE

Pursuant to Federal Rule of Appellate Procedure 32(a)(7)(C) and Third Circuit Rule 31.1(c), the undersigned hereby certifies:

1. Exclusive of the portions exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii), the brief contains 13,802 words according to the word count feature of the word processing software used to prepare the brief.

2. The brief complies with the type size and typeface requirements of Federal Rule of Appellate Procedure 32(a)(5)-(6).

3. The text of the electronic brief is identical to the text in the paper copies.

4. The Sophos Endpoint Security and Control, version 10.3, virus detection program has been run on the electronic copy of this brief and no virus was detected.

Dated: June 15, 2015 /s/ Colleen Bal

CERTIFICATE OF BAR MEMBERSHIP

Pursuant to Third Circuit Rule 28.3(d), the undersigned hereby certifies that the attorneys whose names appear on this brief are members of the bar of this court.

Dated: June 15, 2015 /s/ Colleen Bal

CERTIFICATE OF SERVICE

Pursuant to Third Circuit Rule 31.1, the undersigned certifies that on June 15, 2015, I caused the foregoing brief to be filed with the Clerk of the Court for the United States Court of Appeals for the Third Circuit by using the appellate CM/ECF system and caused seven (7) copies of the brief to be mailed to the Clerk.

All participants in this action are represented by registered CM/ECF users and will be served by the appellate CM/ECF system.

Dated: June 15, 2015 /s/ Colleen Bal