NOT FOR PUBLICATION

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

IN RE NICKELODEON CONSUMER PRIVACY LITIGATION	**MDL No. 2443 (SRC)**
	Civil Action No. 12-07829
	Civil Action No. 13-03755
	Civil Action No. 13-03729
	Civil Action No. 13-03757
THIS DOCUMENT RELATES TO: **ALL CASES**	**Civil Action No. 13-03731**
	Civil Action No. 13-03756
	OPINION

CHESLER, District Judge

This matter comes before the Court upon the motion by Defendants Viacom Inc. ("Viacom") and Google Inc. ("Google") (collectively "Defendants"), to dismiss the Second Consolidated Class Action Complaint ("SAC") filed by Plaintiffs minor children and their father ("Plaintiffs"). For the reasons set forth in an Opinion dated July 2, 2014 ("the July 2 Opinion"), the Court dismissed with prejudice a number of Plaintiffs' claims. The Court also granted Plaintiffs leave to amend certain of its other theories of relief. Specifically, the Court dismissed without prejudice Plaintiffs' Video Privacy Protection Act ("VPPA") claim against Viacom, and their intrusion upon seclusion and New Jersey Computer Related Offenses ("CROA") claims against both Defendants. The issue now before the Court is whether Plaintiffs have cured the deficiencies in those counts. For the reasons that follow, and for those laid out in the July 2 Opinion, the Court finds that Plaintiffs have not cured the enumerated defects. Accordingly, the Court will grant Defendants' motions to dismiss the SAC with prejudice.

I. BACKGROUND

a. Facts

This is a multidistrict consolidated class action lawsuit, and Plaintiffs are children under the age of thirteen who claim that Defendants Viacom and Google have infringed upon their privacy rights. In its July 2 Opinion, the Court extensively reviewed the factual allegations involved, and the Court incorporates that background into this Opinion. For convenience, the Court will briefly restate the contours of the case. The Court assumes the following to be true for purposes of this motion only.

Viacom runs websites for children, including Nick.com, and it encourages users of those web sites to register profiles on them. Viacom collects information about the users who register, including their gender and birthday, and it then assigns a code name to each user based on that information. Children who register also create names associated with their profiles.

Children can stream videos and play video games on these sites, which creates a record of their gender and birthday, as well as the name of the video they played. Viacom sends this record to Google. Viacom also places a text file called a "cookie" onto Plaintiffs' computers without their consent. Cookies allow Viacom to gather additional information about these users, including their IP address, device and browser settings, and web traffic. Viacom shares this cookie information with Google. Additionally, Viacom allows Google to place its own text file "cookies" on Plaintiffs' computers and to access information from those cookies. This lets Google track certain aspects of Plaintiffs' Internet usage. Google's cookies also assign to each Plaintiff an identifier that is associated with other information Viacom has provided. Both Google and Viacom use all of this gathered information to target Plaintiffs with advertising.

b. Procedural History and the Instant Motions

The Court incorporates by reference the procedural history set forth in its July 2 Opinion. In that Opinion, the Court found some of Plaintiffs' claims to be deficient but potentially curable. Specifically, it held that Plaintiffs' VPPA claim against Viacom failed because the data that Viacom discloses is not "personally identifiable information." It further found that Plaintiffs' CROA claim failed because Plaintiffs had not alleged that they suffered any "business or property" damage. With respect to the intrusion upon seclusion claim, the Court found that Plaintiffs had not alleged an intrusion that would be "highly offensive" to a reasonable person. The Court granted Plaintiffs leave to amend these claims.

In response to the Court's July 2 Opinion, Plaintiffs filed the SAC in September of 2014, alleging certain additional facts which they believe cure the aforementioned deficiencies.

Defendants moved to dismiss on October 14, 2014. In support of their motions, Defendants assert that Plaintiffs' SAC suffers from the same fundamental defects. Namely, they urge that Plaintiffs still fail to allege the disclosure of any personally identifiable information; that there are no new allegations of requisite damages; and that the conduct at issue still falls short of the kind of "highly offensive" behavior that is cognizable under tort law.

Plaintiffs oppose the motions, highlighting new allegations included in the SAC. Specifically, Plaintiffs allege that Google could learn Plaintiffs' actual identities by using a "DoubleClick cookie identifier," and by combining the information Viacom provides it with data it already gathers from its other websites and services. Plaintiffs urge that newly alleged facts render Defendants' conduct "highly offensive" and establish the requisite damages.

II. DISCUSSION

a. Legal Standard

A complaint will survive a motion under Rule 12(b)(6) only if it states "sufficient factual allegations, accepted as true, to 'state a claim for relief that is plausible on its face.'" Iqbal, 556 U.S. at 678 (quoting Bell Atlantic v. Twombly, 550 U.S. 554, 570 (2007)). "A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." Id. (citing Twombly, 550 U.S. at 556). Following Iqbal and Twombly, the Third Circuit has held that to prevent dismissal of a claim the complaint must show, through the facts alleged, that the plaintiff is entitled to relief. Fowler v. UPMC Shadyside, 578 F.3d 203, 211 (3d Cir. 2009). In other words, the facts alleged "must be enough to raise a right to relief above the speculative level[.]'" Eid v. Thompson, 740 F.3d 118, 122 (3d Cir. 2014) (quoting Twombly, 550 U.S. at 555).

While the Court must construe the complaint in the light most favorable to the plaintiff, it need not accept a "legal conclusion couched as factual allegation." Baraka v. McGreevey, 481 F.3d 187, 195 (3d Cir. 2007); Fowler, 578 F.3d at 210-11; see also Iqbal, 556 U.S. at 679 ("While legal conclusions can provide the framework of a complaint, they must be supported by factual allegations."). "Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, will not suffice." Iqbal, 556 U.S. at 678.

The Court will apply these principles to assess whether Plaintiffs have cured the pleading deficiencies in their (1) VPPA claims against Viacom; (2) CROA claims against both Defendants; and (3) intrusion upon seclusion claim against both Defendants.

b. The VPPA Claim Against Viacom

Section 2710(b) of the VPPA establishes the elements needed to state a claim under the statute. The VPPA is violated when a video tape service provider ("VTSP") "knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider[.]" For reasons explained extensively in the July 2 Opinion, nothing on the face of the VPPA or its legislative history suggest that "personally identifiable information" ("PII") includes information such as anonymous user IDs, gender and age, or data about a user's computer. In its July 2 Opinion, the Court found that the IP addresses and other information collected here could not, either individually or in the aggregate, identify a Plaintiff and what video they had watched.

The issue is whether Plaintiffs have alleged new facts which make it plausible that the information collected does indeed identify Plaintiffs. The Court finds that they have not.

Plaintiffs argue that because of Google's ubiquitous presence on the Internet, it can learn a lot from even limited information. Plaintiffs note that Google owns a vast network of services -- including Google.com, Gmail, YouTube, and so forth -- which collects ample data about users of those services, sometimes including their full names. Plaintiffs contend that with that information already in hand, Google can take the information Viacom sends it and indeed ascertain personal identities.

The Court has already concluded, however, that PII "is information which must, without more, itself link an actual person to actual video materials." In re Nickelodeon Consumer Privacy Litig., No. 12-cv-7829, 2014 WL 3012873, at *10 (D.N.J. July 2, 2014). Nothing in the amended Complaint changes the fact that Viacom's disclosure does not -- "without more" -- identify individual persons. Id.; see also Ellis v. Cartoon Network, Inc., No. 1:14-cv-484-TWT,

2014 WL 5023535, at *3 (N.D. Ga. Oct. 8, 2014) (quoting In re Hulu Privacy Litigation, No. C-11-03764-LB, 2014 WL 1724344, at *13 (N.D.Cal. Apr. 28, 2014) ("The emphasis is on disclosure, not comprehension by the receiving person.").

Even if the Court were to consider what Google could do with the information, rather than the nature of the information itself, Plaintiffs' claim would still fail because it is entirely theoretical. According 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. Crucially, however, Plaintiffs have alleged no facts whatsoever that a Plaintiff ever registered with Google. Such an allegation is necessary for the theoretical combination of information to actually yield one of the Plaintiff's identities. It appears that Google would not even allow a child under the age of thirteen to register for its services, which would rule out the entire class of Plaintiffs, all of whom are under that age.

At bottom, 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. In that respect, Plaintiffs' VPPA claim resembles one that another court rejected as deficient:

> Although ESPN could be found liable under the VPPA for disclosing both "a unique identifier and a correlated look-up table" by which Plaintiff could be identified as a particular person who watched particular videos, Plaintiff does not allege sufficient facts to support his theory that Adobe already has a "look-up table." Even if Adobe does "possess a wealth of information" about individual consumers, it is speculative to state that it can, and does, identify specific persons as having watched or requested specific video materials from the WatchESPN application.
>
> [Eichenberger v. ESPN, No. 2:14-cv-00463-TSZ (W.D. Wash. Nov. 24, 2014) (Docket Item 38 at 2) (minute order dismissing complaint) (internal citation omitted)].

Here too, the SAC does not allege that Google actually "can, and does, identify" any of the Plaintiffs. The theory upon which Plaintiffs rely to cure this claim is thus wholly speculative. The Court will dismiss Plaintiffs' VPPA claim with prejudice.

c. The CROA Claims Against Both Defendants

The New Jersey CROA is an anti-computer-hacking statute which provides a civil remedy to "[a] person or enterprise damaged in business or property as the result of" certain enumerated actions. N.J. Stat. Ann. 2A:38A-3; see also Marcus v. Rogers, 2012 WL 2428046, at *4 (N.J. App. Div. June 28, 2012) ("This statute plainly requires a plaintiff to prove that he or she was 'damaged in business or property.'").

The Court notes at the outset, as it did in its July 2 Opinion, that because the CROA targets computer hacking, it is dubious whether the law also covers situations like this, in which Plaintiffs' computers have not been hacked nor has their information been stolen. Cf. Mu Sigma, Inc. v. Affine, Inc., No. 12-1323 (FLW), 2013 WL 3772724, at *10 (D.N.J. July 17, 2013) (finding CROA claim deficient in part because it did "not specify how or whether Defendants allegedly stole its data or what in particular was stolen"). By relying upon another statute that does not appear apt to the circumstances, Plaintiffs again seek to fit square pegs into round holes.

Even assuming that the statute applies, the Court earlier dismissed the CROA claim because Plaintiffs failed to allege "business or property" damage stemming from Defendants' conduct. The Court found that just because Defendants could monetize Plaintiffs' Internet usage did not necessarily mean that Plaintiffs could do the same. In the SAC, Plaintiffs now rhetorically frame their damages in terms of unjust enrichment in a quasi-contractual setting. Despite the new semantics, Plaintiffs are pointing to the same exact concept in an attempt to

satisfy the damages requirement. The Court again rejects comparisons between this scenario and unjust enrichment or a quasi-contract, for reasons stated in the July 2 Opinion.

In relevant part, Plaintiffs fail to allege that they could have monetized the PII collected, or if they could, that Defendants' conduct prohibited them from still doing so. See In re Google Cookie Placement Consumer Privacy Litig., 988 F. Supp. 2d 434, 442 (D. Del. 2013) ("[The Complaint] details that online personal information has value to third-party companies and is a commodity that these companies trade and sell . . . . [Yet] plaintiffs have not sufficiently alleged that the ability to monetize their PII has been diminished or lost by virtue of Google's previous collection of it."); see also Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1028-30 (N.D. Cal. 2012) (rejecting allegations that the unauthorized taking of consumer information constitutes injury or damages under other theories of relief).

Plaintiffs have again failed to identify any property or business damage, as is required. Cf. Chance v. Ave. A, Inc., 165 F. Supp. 2d 1153, 1159 (W.D. Wash. 2001) ("Unlike a computer hacker's illegal destruction of computer files or transmission of a widespread virus which might cause substantial damage to many computers as the result of a single act, here the transmission of an internet cookie is virtually without economic harm."). The Court will accordingly dismiss the CROA claim with prejudice.

d. The Intrusion Upon Seclusion Claims Against Both Defendants

New Jersey recognizes "intrusion upon seclusion," a common law privacy tort. Soliman v. Kushner Cos., 77 A.3d 1214, 1224 (N.J. App. Div. 2013) (quoting Hennessey v. Coastal Eagle Point Oil Co., 609 A.2d 11, 17 (N.J. 1992)). That claim imposes civil liability upon one "who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his

private affairs or concerns . . . if the intrusion would be highly offensive to a reasonable person." Hennessey, 609 A.2d at 17 (quoting Restatement (Second) of Torts, § 652B) (emphasis added); see also Castro v. NYT Television, 895 A.2d 1173, 1177 (N.J. App. Div. 2006) (quoting same).

Although the question of what constitutes "highly offensive" conduct is sometimes appropriate for juries, see Vurimindi v. Fuqua Sch. of Bus., 435 F. App'x 129, 136 (3d Cir. 2011) (finding that claim should have survived pleading stage), courts are also empowered to make that determination if it can be decided as a matter of law. Boring v. Google, 362 F. App'x 273, 279 (3d Cir. 2010) ("[Plaintiffs] suggest that the District Court erred in determining what would be highly offensive to a person of ordinary sensibilities at the pleading stage, but they do not cite to any authority for this proposition. Courts do in fact, decide the 'highly offensive' issue as a matter of law at the pleading stage when appropriate.") (citing Diaz v. D.L. Recovery, 486 F.Supp.2d 474, 475–80 (E.D.Pa.2007)).

Here, as in the July 2 Opinion, the Court finds as a matter of law that Defendants' alleged conduct falls short of the "highly offensive" behavior which is cognizable under this theory. Plaintiffs suggest that additional facts pleaded in the SAC render Defendants' conduct "highly offensive" in light of social norms. Specifically, they urge that Defendants' activities violated various statutes and public opinion as expressed through polling.

With respect to the alleged statutory violations, the Court has already determined that Defendants' conduct does not violate the statutes upon which Plaintiffs rely. With respect to public polling, Plaintiffs cite to sentiments that are not directly on point. Plaintiffs highlight, for example, statistics suggesting that a large majority of the public opposes tracking children's online activity. Yet such a statistic does not answer the relevant inquiry: what a reasonable

person finds "highly offensive." That which the public generally supports or opposes does not equate to that which an ordinarily reasonable person finds "highly offensive." Indeed, 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." The Court therefore finds Plaintiffs' polling allegations inapposite to the legal issue. It may indeed strike most people as undesirable that companies routinely collect information about anonymous web users to target ads in a more sophisticated way; yet this theory of relief requires more. See Rush v. Portfolio Recovery Associates, 977 F. Supp. 2d 414, 433 n.23 (D.N.J. 2013) ("[A]n intrusion on seclusion claim requires a showing of conduct more offensive than that which merely annoys, abuses, or harasses.").

Surveying the classic intrusion-upon-inclusion claims demonstrates that this tort supports allegations of truly exceptional conduct. See, e.g., Leang v. Jersey City Bd. of Educ., 198 N.J. 557, 589-90 (2009) (coworker falsely reported that teacher threatened students' lives, causing teacher to undergo psychiatric evaluation); Soliman v. Kushner Cos., 77 A.3d 1214, 1218 (N.J. App. Div. 2013) (defendants hid video recording equipment in bathrooms); Del Mastro v. Grimado, No. BER-C-388-03E, 2005 WL 2002355 (N.J. Super. Ct. Ch. Div. Aug. 19, 2005) (plaintiff's ex-boyfriend distributed erotic photos of her without permission). The Court finds that the collection and disclosure of anonymous browsing history and other similar information falls short of that kind of "highly offensive" behavior. See, e.g., In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (finding unauthorized disclosure of mobile device information to not be egregious breach of social norms); Low v. LinkedIn Corp., 900 F. Supp. 2d 1010, 1025 (N.D. Cal. 2012) (finding disclosure of LinkedIn data insufficiently offensive).

In a final effort to salvage this claim, Plaintiffs urge that the Court should consider Defendants' conduct "highly offensive" because it involves children. It is, of course, apparent to the Court that children do indeed warrant special attention and heightened protections under our laws and social norms. To be sure, however, the Court's role in this decision is not to pass on the morality nor the wisdom of companies tracking the anonymous web activities of children for advertising purposes. The Court does not, by way of this Opinion, find Defendants' conduct beneficial. The Court's only task is to assess whether Plaintiffs' claims pass muster under the federal pleading standards vis-à-vis the authorities upon which those claims rest. Here, Plaintiffs' SAC is an exercise in attempting to fit square pegs into round holes. Although Plaintiffs have identified conduct that may be worthy of further legislative and executive attention, they have not cited any existing and applicable legal authority to supports their claims.

III. CONCLUSION

For the foregoing reasons, the Court will grant Defendants' motions to dismiss [Docket Entries 77 & 78]. An appropriate form of Order will be filed herewith.

s/ Stanley R. Chesler
STANLEY R. CHESLER
United States District Judge

Dated: January 20th, 2015