NOT FOR PUBLICATION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: THE CONSOLIDATION ACTION	**Civil Action No. 13-03731**
	Civil Action No. 13-03756
	OPINION

CHESLER, District Judge

The Plaintiffs in this multidistrict consolidated class action lawsuit are children younger than thirteen who allege that Defendants Viacom Inc. and Google Inc. ("Viacom" and "Google" and, collectively "Defendants") have violated their privacy rights, in contravention of federal law and the laws of California and New Jersey. This matter is before the Court on the Defendants' motions to dismiss the Master Consolidated Class Action Complaint ("MCC"), filed pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6). [Docket Entries 43 & 44.] Plaintiffs have opposed [Docket Entry 52], and the Court has opted to rule on the parties' submissions, and without oral argument. See Fed. R. Civ. P. 78. For the foregoing reasons, the Court finds that the MCC fails to state a claim upon which relief can be granted. Counts II, III, IV, and VII are dismissed with prejudice. Count I is dismissed with prejudice as to Google, and without prejudice as to Viacom. Counts V and VI are dismissed without prejudice as to both Defendants.

I. Background

Viacom owns and operates three websites geared towards children – Nick.com, Nickjr.com, and Neopets.com. Viacom "encourage[s]" users of these websites to "register and establish profiles" on these sites. (See MCC ¶ 85.) Viacom collects certain information about users who register on its sites, including gender and birthdate; Viacom then assigns a code name to each discrete user based on that user's gender and age – allegedly called (by Viacom internally) the "rugrat" code. (Id. at ¶ 89).[1] Children who register for accounts on Viacom's sites also create "unique" profile names that are tied to each child's "profile page." (Id. at ¶ 90.) Each named Plaintiff in this consolidated action is a registered user of one or more of the Viacom websites. (See id. at ¶ 4.)

Children who use these Viacom websites can stream videos or play video games on them – it is unclear from the MCC whether a user must be registered on a Viacom site before watching a video or playing a game. Nevertheless, the MCC alleges that the act of viewing a video or playing a video game creates an "online record," which Viacom collects and later disseminates to Google, who collects and compiles it. (See id. at ¶¶ 96-101.) According to the MCC, the "video viewing" record is a long string of alphanumeric characters that contains two relevant pieces of information – the name of the video "requested" by the website user and the "rugrat" code that describes the age and gender of the user. (See id. at ¶¶ 98-99.)

Before all of this happens, however, Viacom has placed a text file – the aforementioned "cookie" – on Plaintiffs computers; this is done without Plaintiffs consent, or the consent of their

[1] "Rugrat" is both a colloquial term for a child or toddler and also the name of an animated television series that aired on Nickelodeon in the 1990s and 2000s. The rugrat codes provided as examples in the MCC – "Dil," for a six-year-old boy, and "Lou," for a twelve-year-old boy – are names of characters from that show.

parents. (Id. at ¶ 72.) This cookie allows Viacom to acquire certain information – in addition to username, gender, and birthdate collected at the time of registration – about each Plaintiff "who [is] a registered user of Viacom's children's websites." (See id. at ¶ 81.) This information includes a Plaintiff's: "IP address"; "browser settings"; "unique device identifier"; "operating system"; "screen resolution"; "browser version"; and certain "web communications," specifically "detailed URL [Uniform Resource Locator] requests and video materials requested and obtained from Viacom's children's websites." (Id. at ¶ 81.)[2] The MCC alleges that Viacom shares this information with Google, apparently by allowing Google to access the information "contained within Viacom's first party cookies." (See id. at ¶ 75, 81.)

Contemporaneously, Viacom also "knowingly permit[s]" Google to place its own text files – so-called "third-party cookies" – on Plaintiffs' computers; in the alternative, Viacom allows Google to access the information already stored within "third-party cookies" Google may have previously deposited on the device. (Id. at ¶ 73.) Either way, the MCC alleges that Viacom somehow affirmatively authorizes Google's use of cookies to track certain of Plaintiffs' internet usage. The fruits of Google's data tracking include "the URLs . . . visited by the Plaintiffs, the Plaintiffs' respective IP addresses and each Plaintiff's [sic] browser setting, unique device identifier, operating system, screen resolution, browser version, detailed video viewing histories and the details of their Internet communications with" the Viacom sites. (Id. at ¶ 77.) Google's cookies also assign to each Plaintiff a "unique numeric or alphanumeric identifier" that becomes "connected to" the information Viacom discloses to Google about that Plaintiff – namely, the username, gender, birthdate, IP address, etc. (See id. at ¶ 82.) The information is used by Google for the same reason that Viacom uses it -- "to sell targeted advertising" based upon

[2] As described in the MCC, a URL is the address of a resource connected to web, such as a video file. (See MCC ¶ 78.)

Plaintiffs' "individualized web usage, including videos requested and obtained." (See id. at ¶ 84.)

In summary, the MCC alleges that Plaintiffs visit certain Viacom-owned websites and willingly provide Viacom with their gender and age when they register as users of the sites. While this is happening, Viacom places a text file ("cookie") on Plaintiffs' computers without their consent or that of their parents; this text file allows Viacom to collect certain information about the computer that the Plaintiff is using and what the Plaintiff does while on Viacom's website. This information is shared with Google, or at minimum Google is allowed to access the Viacom text file containing it. In addition to the sharing of information from Viacom to Google, Google is also collecting information about Plaintiffs by virtue of its own text files, which Google has placed onto Plaintiffs' computers – again, without their consent – at the behest of (or aided by) Viacom. These "cookies," much like Viacom's, allow Google to collect certain information about Plaintiffs' computers and their website viewing history. Finally, if a registered user watches a video on one of the Viacom websites, Viacom makes a record of that activity, which includes the name of the video watched and the age and gender of the viewer. This information is then shared with Google, who compiles it with similar previously collected information about that particular child.

As the Court reads the MCC, that is the factual basis of the misconduct alleged.[3] Against this backdrop, the MCC alleges seven causes of action. The first three are violations of federal

[3] The Court cannot in connection with this motion credit the allegations made in Paragraphs 66 and 83, which without factual support both state "upon information and belief" that Viacom and Google were able to link online activity and information with offline activity and information, and thereby "identify specific users." (See MCC ¶ 66; see also id. at ¶ 83 ("Defendants . . . were able to identify specific individuals and connect online communications and data . . . to offline communications and data.").) These statements are entirely conclusory, and therefore of little utility in response to a motion to dismiss for failure to state a claim. See Bistrian v. Levy, 696

statutes – the Video Protection and Privacy Act ("VPPA"), 18 U.S.C. § 2710; The Federal Omnibus Crime Control and Safe Streets Act of 1968 ("the Wiretap Act"), as amended by the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. §§ 2510-2522; and the Stored Communications Act ("SCA"), 18 U.S.C. §§ 2701-2712. The other four are state law causes of action based upon the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 631; New Jersey's Computer Related Offenses Act ("CROA"), N.J. Stat. Ann. §§ 2A:38A-1 to -6; invasion of privacy under New Jersey law based on intrusion upon seclusion; and unjust enrichment under New Jersey law.[4] Jurisdiction is therefore exercised pursuant to 28 U.S.C. § 1331, 28 U.S.C. § 1367, and the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2), because the MCC pleads minimum diversity and an amount in controversy greater than $5 million. (MCC ¶ 21.)[5] The MCC defines two Plaintiff classes: (1) a "U.S. Resident Class" comprised of children who visited the Viacom websites and had cookies placed on their computers by Viacom and Google;

F.3d 352, 365 (3d Cir. 2012) ("[W]e peel away those allegations that are no more than conclusions and thus not entitled to the assumption of truth."); Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009). There are simply no facts pleaded in the MCC which indicate when or how either Defendant linked the online information it collected with extra-digital information about the Plaintiffs.

[4] The MCC does not specify which state's law applies to the intrusion upon seclusion and unjust enrichment torts. Plaintiffs, perhaps wary of the maxim that a complaint cannot be amended by a brief opposing a motion to dismiss, undertake an abridged choice of law analysis to support their conclusion that New Jersey law governs the tort claims. (See Opp. Br. at 55-57.) This conclusion was unclear from the MCC itself, because New Jersey law does not generally recognize an independent "unjust enrichment" cause of action. See, e.g., Goldsmith v. Camden County Surrogate's Office, 975 A.2d 459, 462-63 (N.J. Super. Ct. App. Div. 2009) (stating that an unjust enrichment principle normally underpins "a claim of quasi-contractual liability" (quoting Nat'l Amusements, Inc. v. New Jersey Tpk. Auth., 619 A.2d 262 (N.J. Sup. Ct. Law Div. 1992))).

[5] Neither Viacom nor Google challenge the assertion of CAFA jurisdiction over this action. Because CAFA provides the Court with an independent basis for subject matter jurisdiction over this lawsuit, the Court cannot decline pendent jurisdiction over the state law claims. (See Viacom Mov. Br. at 32.)

and (2) a "Video Subclass" comprised of all of the children in the Resident Class who were also registered users of the Viacom websites, "engaged with one or more video materials on such site(s)," and had their "video viewing histories" disclosed to Google by Viacom. (MCC ¶ 103.) The VPPA claim is brought on behalf of the Video Subclass only; all other counts are brought on behalf of the Resident Class.

II. Whether Plaintiffs Have Standing to Sue

Both Defendants raise a threshold argument that Plaintiffs have no standing under Article III of the Constitution to bring this suit. (Viacom Mov. Br. at 12; Google Mov. Br. at 11-14.) The "irreducible constitutional minimum of standing contains three elements" – injury-in-fact, causation, and redressability. See Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992); Danvers Motor Co., Inc. v. Ford Motor Co., 432 F.3d 286, 290-91 (3d Cir. 2005). Defendants have not challenged causation and redressability here; rather, Defendants focus their argument exclusively on injury-in-fact, and in particular on whether or not the MCC plausibly alleges that Plaintiffs were economically harmed by Defendants' collection of their personal information. (See, e.g., Viacom Mov. Br. at 13-14.) Defendants contend that it does not, and because Plaintiffs have suffered no economic injury – a "paradigmatic" or "classic" form of injury-in-fact, see Danvers, 432 F.3d at 291, 293 – the MCC must be dismissed for lack of standing.

Were it necessary to decide the question, the Court might be inclined to agree. The MCC describes at some length why the personal information collected and aggregated by Defendants has a pecuniary value to companies who monetize popular websites by selling targeted advertising on those sites. (See, e.g., MCC ¶ 49 ("To the advertiser, targeted ads provided [sic] an unprecedented opportunity to reach potential consumers. The value of the information that

Defendants take from people who use the Internet is well known . . . . Personal information is now viewed as a form of currency.").) Even assuming this proposition to be true, it does not follow that personal information of the type collected by Viacom and Google has actual monetary value to Plaintiffs themselves, a fact necessary to Plaintiffs' theory of economic injury. (See Opp. Br. at 12 ("The [MCC] alleges a violation of Plaintiffs' financial interests to support their allegations that personally identifiable information . . . has monetary value and is a commodity . . . .").) In other words, the MCC presupposes the proposition that Plaintiffs could sell their personal information if they wanted to because Viacom and Google might already do so. In the parlance of standing, this theory is "abstract or conjectural or hypothetical," and therefore not "legally . . . cognizable." See Danvers, 432 F.3d at 291. It is also indistinguishable from 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. See In re DoubleClick, Inc. Privacy Litig., 154 F. Supp. 2d 497, 525 (S.D.N.Y. 2001) ("Demographic information is constantly collected on all consumers by marketers, mail-order catalogues and retailers. However, we are unaware of any court that has held the value of this collected information constitutes damage to consumers or unjust enrichment to collectors.")

But whether or not Plaintiffs have alleged injury-in-fact in the form of economic harm is not dispositive to the standing analysis. Injury-in-fact is nothing more or less than an "invasion of a legally protected interest which is . . . concrete and particularized . . . [and] actual or imminent, not conjectural or hypothetical." Pichler v. UNITE, 542 F.3d 380, 390 (3d Cir. 2008) (quoting Lujan, 504 U.S. at 560-61). The "legally protected interest" can be – and often is – property-based or financial. But it need not be. See Alston v. Countrywide Financial Corp., 585

F.3d 753, 763 (3d Cir. 2009) (addressing standing under the federal Real Estate Settlement Procedures Act and stating that "[a] plaintiff need not demonstrate that he or she suffered actual monetary damages"). Indeed, it has long been the case that "[t]he actual or threatened injury required by Art. III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing . . . ." See Warth v. Seldin, 422 U.S. 490, 500 (1975) (internal quotation and marks omitted); see also Pichler, 542 F.3d at 390-91. Thus, where a plaintiff states a valid claim for violation of an individual right or set of rights conferred via statute the issue of monetary harm is generally superfluous to the standing inquiry. This is why the Third Circuit has both explicitly and implicitly treated inquiries into statutory standing and whether a statutory claim has been stated as one and the same. Baldwin v. Univ. of Pittsburgh Med. Ctr., 636 F.3d 69, 73 (3d Cir. 2011) ("A dismissal for lack of statutory standing is effectively the same as a dismissal for failure to state a claim."); Pichler, 542 F.3d at 390-91 (affirming dismissal for lack of standing where plaintiffs did not meet the definition of "individual" under the Drivers Protection Privacy Act, 18 U.S.C. §§ 2721-2725, and thus had no cause of action).

In short, if Plaintiffs can state valid claims for violations of statutes that codify certain of their privacy rights, the Court will not prevent Plaintiffs from suing to enforce those rights because of doubts about whether they have suffered concrete monetary harm. Cf. In re Google Inc. Cookie Placement Consumer Privacy Litig., 2013 WL 5582866, at *3 (D. Del. Oct. 9, 2013) ("Google Cookie") (concluding that complaint based upon placement of Google third-party cookies did not allege sufficient injury-in-fact but proceeding to analysis of "whether plaintiffs have pled sufficient facts to establish a plausible invasion of rights created by the various statutes asserted"); In re Zynga Privacy Litig., No. 10-cv-04680, 2011 WL 7479170, at *2 (N.D. Cal.

June 15, 2011) ("Plaintiffs have Article III standing, because they allege a violation of their statutory rights under the Wiretap Act."), aff'd, -- F.3d --, 2014 WL 1814029 (9th Cir. May 8, 2014). Consequently, the Court must now turn to Defendants' argument that the facts alleged in the MCC do not state claims for violations of the various statutes asserted.[6] If Defendants are correct, any need to revisit the standing question will be rendered unnecessary. See Alston, 585 F.3d at 758 (addressing "lingering" Article III concerns only after determining that plaintiffs had stated a claim under the Real Estate Settlement Procedures Act).

III. Whether The MCC States A Plausible Claim for Relief

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.

[6] Viacom invites the Court to follow Sterk v. Best Buy Stores, L.P., No. 11 C 1894, 2012 WL 5197901 (N.D. Ill. Oct. 17, 2012), and hold that Plaintiffs are required to plead "an injury beyond a statutory violation" to have standing. (Viacom Reply Br. at 6 n.1.) The Court must decline. Insofar as Sterk holds that pleading a violation of a statutory right without more is not an injury-in-fact, the case is incompatible with binding Third Circuit authority. See Alston, 585 F.3d at 763; Pichler, 542 F.3d at 390 (basing standing analysis on whether plaintiffs suffered "an invasion of a legally protected interest" created by the DPPA). Such inconsistency notwithstanding, the Court agrees with the In re Hulu Privacy Litigation Court's characterization of Sterk as a case of limited persuasive authority which is best understood in context. See No. C 11-03764, 2013 WL 6773794, at *8 (N.D. Cal. Dec. 20, 2013) (noting that Sterk found no VPPA injury where defendants Best Buy Stores, L.P. and BestBuy.com LLC only disclosed plaintiff's "DVD purchase history and other information to their parent company, Best Buy Co., Inc." (citing 2012 WL 5197901, at *1-3, *5)).

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.

B. The VPPA Claim Against Google

Whether the MCC states a claim against either Viacom or Google for violation of the federal VPPA is a question of statutory interpretation. See In re Hulu Privacy Litig., 2014 WL 1724344, *6-7 (N.D. Cal. Apr. 28, 2014). The Court will therefore address the merits of certain of Defendants' text-based arguments, starting with Google's contention that it is not a "video tape service provider" within the ambit of the VPPA, and thus as a matter of law could not have violated Plaintiffs' rights under that statute. (See Google Mov. Br. at 28-29.)

1. Only VTSPs Can be Civilly Liable for Violations of the VPPA, and the MCC Does Not Allege that Google is A VTSP

It is well established that "every exercise of statutory interpretation begins with an examination of the plain language of the statute." United States v. Diallo, 575 F.3d 252, 256 (3d Cir. 2009) (quoting Rosenberg v. XM Ventures, 274 F.3d 137, 141 (3d Cir. 2001)). 18 U.S.C. § 2710(b), entitled "Video tape rental and sales records," provides that "[a] video tape service provider who knowingly discloses, to any person, personally identifiable information concerning

any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection [(c)]."[7] Section 2710(c), entitled "Civil action," states that "[a]ny person aggrieved by an act of a person in violation of this section may bring a civil action in a United States district court." Reading these two provisions together, the Act limits the right to sue to those persons "aggrieved" by "violation[s] of" the VPPA itself, and the VPPA is violated when a "video tape service provider . . . knowingly discloses . . . personally identifiable information concerning" that "aggrieved" person. It is thus apparent on the face of the VPPA that an "aggrieved" person's claim must be against a "video tape service provider" ("VTSP"). The great majority of courts to address the issue have reached the same conclusion. See, e.g., Daniel v. Cantrell, 375 F.3d 377, 381, 82 (6th Cir. 2004) ("[U]nder the plain language of the statute, only a 'video tape service provider' . . . can be liable."); Hulu, 2014 WL 1724344, at *7 ("[t]he VPPA prohibits a 'videotape service provider' from" knowingly disclosing "personally identifiable information" (citing § 2710(b))).

Plaintiffs contend otherwise. Relying exclusively on Dirkes v. Borough of Runnemede, 936 F. Supp. 235 (D.N.J. 1996), Plaintiffs argue that any party who is "in possession of personally identifiable information as a direct result of the improper release of such information" is subject to VPPA liability. (Opp. Br. at 22 (quoting Dirkes, 936 F. Supp. at 240).) According to Plaintiffs, the Dirkes decision establishes a "law" of the District of the New Jersey, and thus in this district VPPA liability is not limited to VTSPs only. (See Opp. Br. at 22, 24 ("this Court should follow the law of this district" (citing Dirkes, 936 F. Supp. at 239)).) There is, however,

[7] The actual text of the VPPA says that "such provider shall be liable to the aggrieved person for the relief provided in subsection (d)." § 2710(b). This appears to be a typo, because subsection (d) is a rule of evidence which renders inadmissible personally identifiable information, whereas subsection (c) describes the remedies available to a VPPA plaintiff in a civil action. See Sterk v. Redbox Automated Retail, LLC, 672 F.3d 535, 537 (7th Cir. 2012).

no such thing as "law of the district," and "[t]he doctrine of *stare decisis* does not compel one district court judge to follow the decision of another," even where the facts of the two cases are the same. Threadgill v. Armstrong World Indus., Inc., 928 F.2d 1366, 1371 (3d Cir. 1991). While the Court has the highest regard for the author of the Dirkes opinion, the Court is not persuaded that Dirkes correctly interprets the relevant VPPA provisions.

Instead, the Court agrees with the Sixth Circuit's discussion in Daniel that Dirkes reaches the holding it does – *i.e.*, that persons other than VTSPs can be liable under the VPPA – based on a misreading of the statute. See Daniel, 375 F.3d at 382-83. Dirkes appears to be based upon the false premise that "the plain language of the [VPPA] does not delineate those parties against whom an action under this Act may be maintained." See 936 F. Supp. at 240. This is simply not the case. Certainly, subsection (c) – which Dirkes focuses on but puzzlingly reads in isolation – does not explain who can be liable in a VPPA suit; and that makes sense, because subsection (c) deals exclusively with the victims of the conduct denounced by the statute. See § 2710(c) ("[a]ny person aggrieved by an act of a person in violation of this section may bring a civil action"). Elsewhere, however, the VPPA does explain "those parties" who can be sued under the Act – namely, VTSPs. See § 2710(b) ("a [VTSP] . . . shall be liable to the aggrieved person"). Thus, it is only by ignoring the very subsection that establishes the contours of a VPPA cause of action that Dirkes concludes that the possible universe of VPPA defendants is infinite. See 936 F. Supp at 240 (finding that the court "need not identify all potential categories of defendants in this opinion").

Moreover, Dirkes understands Congress to be granting to federal judges "broad remedial powers" to remedy VPPA violations because the Act states that "[t]he court may award . . . such

other . . . relief as the court determines to be appropriate." See 936 F. Supp. at 241 (quoting 18 U.S.C. § 2710(c)(2)(D)). Dirkes chooses to exercise those powers by expanding the scope of permissible VPPA defendants, "to prevent the further disclosure of information." See id. But again, this is contrary to the plain language of the VPPA itself. The "such other . . . relief" language describes the type of remedy – like statutory damages and attorneys' fee – that "[t]he court may award"; it does not indicate against whom such relief may be awarded. That indication comes from § 2710(b), which states that a VTSP "who knowingly discloses . . . personally identifiable information concerning any consumer . . . shall be liable" to that person.

In short, as the Sixth Circuit correctly highlights Congress provides a detailed definition of a VTSP in § 2710(a) and makes the cause of action created in § 2710(b) contingent on actions taken by VTSPs; it does violence to this plain language to read § 2710(c) in isolation and conclude that anyone can violate the statute. See Daniel, 375 F.3d at 383. This Court, fortified by the Sixth Circuit's persuasive analysis in Daniel, therefore holds that only VTSPs can be liable for violations of the VPPA.

Having determined that only VTSPs can violate the VPPA, the Court finds that the VPPA claim against Google must be dismissed because the MCC does not allege Google is a VTSP. According to the VPPA, a VTSP is a person "engaged in the business . . . of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials, or any person or other entity to whom a disclosure is made under subparagraph (D) or (E) of subsection (b)(2), but only with respect to the information contained in the disclosure." By referencing these two subparagraphs, the statute broadens the definition of VTSP to include: (1) "any person if the disclosure [of information by the VTSP] is solely of the names and addresses of consumers and

if" certain other factors are met, see § 2710(b)(2)(D); and (2) "any person if the disclosure is incident to the ordinary course of business of the video tape service provider," see § 2710(b)(2)(E). Notably, the term "ordinary course of business" is defined to include "only debt collection activities, order fulfillment, request processing, and the transfer of ownership." § 2710(a)(2).

None of these definitions fit Google here. The MCC does not allege that Google is "engaged in the business" of renting, selling, or delivering either video tapes or "similar audio materials" – instead, it describes Google as (1) the global epicenter of Internet search and browsing activity"; (2) an "advertising company"; and (3) an "[e]nterprising online marketer[]" who utilizes its third-party cookies "to sell advertising that is based upon a particular person's prior Internet activity." (See id. at ¶¶ 19, 35, 37.) Moreover, Google is not a VTSP by virtue of the alleged disclosures made to it by Viacom – the MCC does not allege that the disclosures made to Google are "solely . . . the names and addresses of consumers," see § 2710(b)(2)(D), and it does not allege that the disclosures are made in the "ordinary course of [Viacom's] business," as that term is defined in the statute. See id. §§ 2710(a)(2), 2710(b)(2)(E).

Plaintiffs contend that, despite what the MCC alleges (or fails to allege), Google is in fact a VTSP because it owns YouTube, a provider of "[o]nline video services" that is considered to be a VTSP "within the meaning of the VPPA." (See Opp. Br. at 25 (quoting Hulu, 2012 WL 328296, at *4-6).) Even if this is true, "after-the-fact allegations" like these, which are contained in a brief filed in opposition to a motion to dismiss but not in the complaint itself, do not factor into the Rule 12(b)(6) analysis. See Frederico v. Home Depot, 507 F.3d 188, 201-02 (3d Cir.

2007). Thus, the MCC is still deficient on this score, regardless of how Plaintiffs characterize Google in their brief.

But even if Plaintiffs were given leave to amend the MCC so they could allege Google is a VTSP because of its ownership of YouTube, it would not help. The presence of "personally identifiable information," defined at 18 U.S.C. § 2710(a)(3) and discussed in greater detail *infra*, is a mandatory prerequisite to a cognizable VPPA suit. "Personally identifiable information," however, is contingent on the request or receipt of "specific video material or services from a [VTSP]." See § 2710(a)(3). Thus, the VPPA only contemplates civil actions against those VTSP from whom "specific video materials or services" have been requested. It is readily apparent that is not the case with Google here, nor could it ever be – YouTube videos are irrelevant to this lawsuit, which focuses exclusively on three Viacom websites and the Defendants' data collection activities in regards to those sites. The VPPA's legislative history confirms that Google's ownership of YouTube does not bring Google within the Act's ambit in this case. See S. Rep. No. 100-599, at 12 (1988) ("Senate Report"), as reprinted in 1988 U.S.C.C.A.N. 4342-1 ("The definition of personally identifiable information includes the term 'video' to make clear that simply because a business is engaged in the sale or rental of video materials or services does not mean that all of its products or services are within the scope of this bill.") As least as far as Google is concerned, this is a lawsuit about online advertising practices, not online videos.

2. 18 U.S.C. § 2710(e) Cannot be the Basis for A Civil Claim Against Google

As the foregoing analysis reveals, only those persons "aggrieved" by an act in violation of the VPPA may bring a civil action, and one can only be "aggrieved" for purposes of the

statute when a VTSP "knowingly discloses" his or her "personally identifiable information." See § 2710(b). Since Plaintiffs have not alleged that Google is a VTSP, they cannot state a VPPA claim against it. Nevertheless, Plaintiffs contend that Google is liable for damages and other relief provided by the Act for a violation of § 2710(e) ("Destruction of old records"), which requires "person[s] subject to [the VPPA]" to timely "destroy personally identifiable information." Plaintiffs' lone allegation in this regard, found in Paragraph 131 of the MCC, is wholly conclusory, and is not supported by any factual allegations whatsoever – for instance, the MCC does not describe how long Google retains Plaintiffs' information, a fact that would seem integral to a suit based upon the failure to destroy "old records." Plaintiffs' VPPA claim against Google, insofar as it is predicated upon § 2710(e), must therefore be dismissed. See Iqbal, 556 U.S. at 678 ("Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, will not suffice.").

More importantly, it is readily apparent that non-compliance with § 2710(e) cannot serve as the basis of a VPPA action. See Daniel, 375 F.3d at 384 ("only § 2710(b) can form the basis of liability"); Redbox, 672 F.3d at 538. While Dirkes holds to the contrary, the Court is satisfied that the reasoning applied in the Daniel and Redbox opinions is more persuasive. Both the Sixth and Seventh Circuits untangle the same statutory text and explain why the placement of the VPPA's civil action provision – immediately following subsection (b)'s disclosure prohibitions, but before the prohibitions contained in subsections (d) and (e) – is not an accident; rather, it is evidence that Congress intended the VPPA's right of action to be "limited to enforcing the prohibition of disclosure." See Redbox, 672 F.3d at 538; Daniel, 375 F.3d at 384 ("If these later sections [subsections (d) and (e)] were to be a basis for liability, it would make sense that the

section on civil actions [subsection (c)] would come at the end of the statute, rather than preceding these sections."). The manner in which the civil action provision is drafted further strengthens this conclusion – subsection (c)(4) states that "[n]o liability shall result from lawful disclosure permitted by this section." It is unclear why Congress would add this caveat – redundant, to be sure, but still there – if it did not intend liability to be limited only to violations of subsection (b), which explains how an unlawful disclosure occurs.[8]

In sum, the Court does not agree with Plaintiffs that § 2710(e) authorizes a civil VPPA action, let alone one against a non-VTSP entity. The VPPA claim against Google, predicated on Google's alleged failure to destroy old records and unsupported by factual allegations, fails as a matter of law and will be dismissed with prejudice.

C. The VPPA Claim Against Viacom

In contrast, the MCC expressly pleads that Viacom is a VTSP within the terms of the statute. (See MCC ¶ 126 ("The home page of Nick.com advertises it as the place to watch '2000+ FREE ONLINE VIDEOS' . . . .").) Viacom makes a tepid attempt to contest this characterization, arguing in a footnote of its moving brief (and a paragraph of the reply) that the VPPA does not apply to entities that stream videos online. (See Viacom Mov. Br. at 19 n.4; Reply Br. at 12-13.) Because, however, the Court finds that the VPPA claim against Viacom must fail for other reasons, it is unnecessary to determine whether or not Viacom is a VTSP by

[8] The VPPA's legislative history, while unnecessary to consult to decide the question, further supports the conclusion that the remedies in subsection (c) are only available for violations of subsection (b). See, e.g., Senate Report at 7 (statement of Sen. Leahy) ("In the event of an unauthorized disclosure, an individual may bring a civil action for damages."); id. at 8 ("The civil remedies section puts teeth into the legislation, ensuring that the law will be enforced by individuals who suffer as the result of unauthorized disclosures."); id. at 14 ("Section 2710(c) imposes liability where an individual, in violation of the act, knowingly discloses personally identifiable information concerning any consumer.").

virtue of its provision of online streaming videos.[9] Specifically, the Court finds merit in Viacom's argument that the VPPA claim fails because the information allegedly acquired and disclosed by Viacom is not "personally identifiable information" as that term is defined by the statute. (Viacom Mov. Br. at 18-20.) In short, there is simply nothing on the face of the statute or in its legislative history to indicate that "personally identifiable information" includes the types of information – anonymous user IDs, a child's gender and age, and information about the computer used to access Viacom's websites – allegedly collected and disclosed by Viacom.

As already discussed, § 2710(b) establishes the elements of a VPPA cause of action; the statue is violated when a VTSP "knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider . . . ." "Personally identifiable information" ("PII") is a defined term – PII "includes information which identifies a person as having requested or obtained specific video materials or services from a [VTSP]." § 2710(a)(3). Quoting this definition, Viacom argues that PII is "information sufficient to identify a person, by real name, in the real world, as having obtained a 'specific video' . . . ." (See Viacom Mov. Br. at 20.) Viacom suggests that "[i]t is clear that Congress had 'the names and addresses of consumers' in mind" when drafting its definition of PII. (See id.)

This reading, however, does not jive with the VPPA's plain language. If Congress wanted to define PII as any "information which identifies a person by name or mailing address as having requested or obtained specific video materials," it could have. Those words, however, are nowhere to be found in the definition. Moreover, subsection (b)(2), which establishes certain

[9] The Court notes that the only other court to address the issue of whether providers of streaming videos are VTSPs has found that they are, at least for pleading purposes. See Hulu, 2012 WL 3282960, at *6 (rejecting argument by online video content provider that "the VPPA does not expressly cover digital distribution" of video materials). Viacom does not suggest a persuasive reason why the Hulu Court's conclusion was incorrect.

exceptions to the prohibition against disclosure, explains that a VTSP "may disclose [PII] concerning any consumer . . . to any person if the disclosure is solely of the names and addresses of consumers and if" certain other factors are met. See § 2710(b)(2)(D). That language implies that "names and addresses" are but a subset of PII; otherwise, why include the "if the disclosure is" clause at all? The Court therefore reads the statute to comport with common sense – "a person" can be identified by more than just their name and address. See Hulu, 2014 WL 1724344, at *11 ("One can be identified in many ways: by a picture, by pointing, by an employee number, by the station or office or cubicle where one works . . . .").

That does not mean the universe of PII is as broad as Plaintiffs suggest either. Indeed, the Hulu decision, which engages in an exhaustive analysis of the VPPA's text and legislative history, holds that PII is information that must link "a specific, identified person and his video habits" – what the Hulu Court characterizes as any information "akin" to a name. See 2014 WL 1724344, at *12, 14. This is a cogent and reasonable reading of the statute, which on its face establishes that PII is "information" that itself must both "identif[y] a person" and further identify that "person" in connection with "specific video materials or services" "requested or obtained" from a VTSP. See § 2710(a)(3). At bottom, then, this Court concludes that PII is information which must, without more, itself link an actual person to actual video materials.

To the extent of any ambiguity in the statute's definition of PII, the VPPA's legislative history comports with this reading. As the parties highlight, the VPPA was passed in direct response to the publication of a newspaper profile about then-Supreme Court nominee Judge Robert Bork based upon the titles of movies he had rented from a local video store. See Senate Report, at 5. This disclosure was resoundingly denounced. In the words of Senator Patrick

Leahy, "[i]t is nobody's business what Oliver North or Robert Bork or Griffin Bell or Pat Leahy" – all identified, specific people – "watch on television or read or think about when they come home." Id. The Senate Report's discussion of PII echoes this emphasis on preventing the dissemination of the video viewing habits of identifiable individuals:

> This definition [of PII] makes clear that personally identifiable information is intended to be transaction oriented. It is information that identifies a particular person as having engaged in a specific transaction with a [VTSP] . . . . Thus, for example, a video tape service provider is not prohibited from responding to a law enforcement agent's inquiry as to whether a person patronized a [VTSP] at a particular time or on a particular date.

Id. at 12. Conspicuously absent from this treatment is any discussion about PII being tied to the actual names or addresses of individuals; but so too is any indication that PII can be anonymous information which may after investigation lead to the identification of a specific person's video viewing habits.

And it is this conclusion that is fatal to the VPPA claim against Viacom. The MCC alleges that Viacom disclosed the following information to Google about each Plaintiff: anonymous username; IP address; browser setting; "unique device identifier"; operating system; screen resolution; browser version; and "detailed URL requests and video materials requested and obtained" from the Viacom websites, requests which presumably contain the "rugrat" (gender and age) code and the title of a video. None of this information, either individually or aggregated together, could without more serve to identify an actual, identifiable Plaintiff and what video or videos that Plaintiff watched. Much of this information – screen resolution, browser version and setting, operating system, etc. – is not even anonymized information about

the Plaintiff himself; it is anonymized information about a computer used to access a Viacom site.

Additionally, Plaintiffs themselves highlight that merely acquiring an IP address does not itself identify an individual – Plaintiffs argue (but do not plead) that "IP addresses are looked up easily to reveal geolocation information." (See Opp. Br. at 20 n.13.) But even "geolocation information" does not identify a specific individual. Indeed, it will often have the opposite effect: to adopt an example used by the parties, the computer on which this Opinion was written is located in Newark, New Jersey, but the IP address associated with it is geographically located in Philadelphia – presumably where the Third Circuit's computer servers are. Knowing anonymized information about a computer, and an IP address associated with that computer, will not link actual people (children or adults) to their specific video choices, any more than knowing that an Opinion was written on an HP Compaq running Windows XP located at a Philadelphia IP address will link an actual judge to a specific case.

The closest the MCC comes is the allegation that Viacom disclosed to Google specific profile names and a URL containing: (1) Viacom's internal "rugrat" code; (2) the name of a specific video; and (3) information identifying a Google "third-party" cookie. (See MCC ¶¶ 98-99.) But even assuming Google knew which codes names where associated with certain age and gender combinations – and the MCC is less than clear on this point[10] – this information does not link an identified person to a specific video choice. Instead, as Plaintiffs themselves highlight, all Google knows from the disclosure of this information (plus the computer specific information

[10] Specifically, the MCC alleges that "Viacom also provided Google with the code name for the child's specific gender and age." (MCC ¶ 93.) This allegation could be read in two ways – Viacom (1) provided Google with a key to decipher the "rugrat" code (*e.g.*, Dil = six-year-old boy), or (2) provided a code name that only Viacom knew corresponded to a specific age and gender.

discussed above) is "a child's username, sex, age, type of computer," and IP address. (See Opp. Br. at 20.) This is simply not information that, without more, identifies a person – an actual, specific human being – as having rented, streamed, or downloaded a given video, especially given the absence of factual allegations regarding how (and if) Plaintiffs' unique usernames were linked to their actual names. Certainly, this type of information might one day serve as the basis of personal identification after some effort on the part of the recipient, but the same could be said for nearly any type of personal information; this Court reads the VPPA to require a more tangible, immediate link.

None of the cases Plaintiffs cite alter this conclusion. Plaintiffs again cite to Dirkes (see Opp. Br. at 16), but Dirkes is inapposite, since it dealt with the disclosure of the plaintiffs' real names and a history of the pornographic videotapes they rented from a local video store. See 936 F. Supp. at 236. This information is so clearly PII that Dirkes, if anything, serves only to illustrate how far Plaintiffs in this case attempt to stretch that term's definition. Plaintiffs also make much out of an earlier decision in the Hulu litigation, in which the court rejected Hulu's motion to dismiss based upon, *inter alia*, the argument that Hulu was not a VTSP within the terms of the VPPA. See 2012 WL 3282960, at *4-8. That decision is also unhelpful. There, Hulu never argued that the type of information it disclosed was not PII, and thus the court in that case did not make any findings about whether the types of information allegedly disclosed by Hulu were PII or not. More importantly, the allegations in Hulu differ in critical ways from those here. The Hulu plaintiffs alleged, among other things, that Hulu transmitted "their Facebook IDs, connecting the video content information to Facebook's personally identifiable user registration information." See id. at *2. No such allegations exist in this case – the closest

the MCC comes is to allege that Viacom gives Google the video viewing histories of anonymous children categorized by age and gender. (See MCC at ¶¶ 98-99.)

The most recent decision in the Hulu litigation, denying in part Hulu's motion for summary judgment, emphasizes just how important the disclosure of Facebook-related identification information was to the survival of the VPPA claim in that case. In that decision, the court analyzed whether any of three different types of disclosures came close enough to "linking identified persons to the video they watched" to resist judgment as a matter of law. The disclosures were: (1) a "URL web address containing the video name and the Hulu user's unique seven-digit Hulu User ID"; (2) a unique user ID that allowed comScore (a company hired to calculate viewership) "to link the identified user and the user's video choices with information . . . gathered from other websites that the same user visited;" and (3) a transmission to Facebook containing information "about what the Hulu user watched and who the Hulu user is on Facebook." See Hulu, 2014 WL 1724344, at *9, *13. The court held that only the last disclosure – which identified the user's "actual identity on Facebook" – was actionable. See id. Critically, the court found that

> a Facebook user – even one using a nickname – generally is an identified person on a social network platform. The Facebook User ID is more than a unique, anonymous identifier. It personally identifies a Facebook user. That it is a string of numbers and letters does not alter the conclusion. Code is a language, and languages contain names, and the string is the Facebook user name.

Id. at 14. None of the allegedly disclosed information in this case – anonymous information about home computers, IP addresses, anonymous usernames, even a user's gender and age – serves to identify an actual, identifiable person and link that person to a specific video choice.

Simply put, in a socially networked world a Facebook ID is at least arguably "akin" to an actual name that serves without more to identify an actual person. This Court, however, need not decide that issue, because the same simply cannot be said about the information allegedly disclosed here.

The fact that Plaintiffs are all minors does not alter the analysis either. Certainly, the ease by which children access the internet implicates important policy concerns, and Congress has legislated in this area, passing the Children's Online Privacy Protection Act ("COPPA"), 15 U.S.C. §§ 6501-6506. But as Viacom highlights, Plaintiffs do not allege that either party has violated COPPA, and considering the broader rulemaking authority granted by Congress to the Federal Trade Commission ("FTC") under COPPA, FTC rules implementing that statute are irrelevant to this Court's VPPA analysis. See § 6501(8)(F) (granting FTC authority to expand statutory definition of "personal information" beyond, *inter alia*, names, address, Social Security numbers, and telephone numbers). The VPPA by its very terms applies equally regardless of the age of the consumer, and nothing in the Act's legislative history indicates any Congressional intent to transform disclosures of non-PII into VPPA violations because the subject of the disclosure is younger than thirteen. See Hulu, 2014 WL 1724344, at *12 (noting that COPPA, which specifically protects children online, "implicates different privacy concerns and resulted in broader definitions of personal information," while "[b]y contrast" "the VPPA prohibits only disclosure of a particular viewer's watched videos").[11]

[11] Also immaterial are certain public statements reproduced in Plaintiffs' opposition brief and attributed to Viacom, in which Viacom announced that YouTube would strip "personally identifiable information" from data before transferring that data to Viacom pursuant to a court order. (See Opp. Br. at 19.) Statements made by Viacom about the anonymity of information disclosed to it by a Google subsidiary say nothing about whether the information allegedly disclosed by Viacom to Google in this case is itself anonymized, or something more nefarious. Insofar as Plaintiffs intend the underlying Viacom/Google copyright litigation to serve as legal

In sum, Plaintiffs do not state a VPPA claim against Viacom because they fail to allege the disclosure of personally identifiable information by Viacom to Google. The VPPA claim against Viacom will be dismissed. This dismissal, predicated upon Plaintiffs' failure to plead facts showing Viacom disclosed PII, will be without prejudice. Phillips v. County of Allegheny, 515 F.3d 224, 236 (3d Cir. 2008) ("where a complaint is vulnerable to a 12(b)(6) dismissal, a district court must permit a curative amendment, unless an amendment would be inequitable or futile").

D. The Wiretap Act Claim

The Wiretap Act creates a civil cause of action "against those who intentionally use or disclose to another the contents of a wire, oral, or electronic communication, knowing or having reason to know that the information was obtained in violation of the statute." Bartnicki v. Vopper, 200 F.3d 109, 114-15 (3d Cir. 1999) (citing 18 U.S.C. §§ 2511(1), 2520(a)). The Third Circuit has held that "private parties can bring a cause of action for damages and injunctive relief where aggrieved by a defendant's . . . unauthorized interception of electronic communications." DIRECTV, Inc. v. Pepe, 431 F.3d 162, 167 (3d Cir. 2005). Plaintiffs allege that Google "intentionally intercepted the contents of [Plaintiffs'] electronic communications" through its placement and use of cookies, while Viacom "procured Google" to so intercept and "profited" from this "unauthorized tracking of the Plaintiffs' Internet communications." (MCC ¶¶ 147, 156-57.) The Wiretap Act claim fails as a matter of law as to both Defendants, and will be dismissed with prejudice.

---

authority, the Court notes that the Opinion and Order which precipitated Viacom's excerpted statement actually supports the Defendants' position. See Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 262 (S.D.N.Y. 2008) (quoting with approval defendants' statement that a "login ID is an anonymous pseudonym that users create for themselves when they sign up with YouTube" which "cannot identify specific individuals" without more).

Indeed, the claim is defective for two distinct reasons. First, Defendants' correctly highlight that the Wiretap Act is a "one-party consent" statute, i.e., it is not unlawful under the Act for a person to "intercept . . . electronic communication" if the person "is [1] a party to the communication or [2] where one of the parties to the communication has given prior consent to such interception . . . ." § 2511(d)(2). Defendants argue that as alleged in the MCC, all communications in this case were either directly between themselves (or their cookies) and Plaintiffs' computers, or intercepted with the express consent of websites like Viacom. (See Viacom Mov. Br. at 25; Google Mov. Br. at 17.)[12]

Plaintiffs do not seriously dispute this. Instead, Plaintiffs attempt to invoke the "criminal or tortious act" exception to the Wiretap Act's one-party consent regime based on the MCC's allegation of a common law privacy tort against Defendants. (See Opp. Br. at 28-29 ("Plaintiffs' allegation of intrusion upon seclusion is sufficient to invoke the tort/crime exception of the [Wiretap Act], and negate the relevance of Viacom's consent."). While Plaintiffs are correct that consent will not absolve liability where a "communication is intercepted for the purpose of committing any criminal or tortious act," see § 2511(2)(d), that exception does not help them here. Courts have almost uniformly found that the "criminal or tortious act" exception applies only where defendant has "the intent to use the illicit recording to commit a tort or crime beyond the act of recording itself." See Caro v. Weintraub, 618 F.3d 94, 98 (2d Cir. 2010); see also

[12] Paragraph 155 of the MCC alleges that Google uses its cookies to "track the Plaintiffs' communications with other websites on which Google places advertisements," "in addition to intercepting the Plaintiffs' communications with the Viacom children's websites . . . ." Plaintiffs contend that this single paragraph "provides a separate and unchallenged basis" for a Wiretap Act claim against Google. (Opp. Br. at 37.) Even if the Court were to credit this conclusory allegation, made with no factual support, it provides no independent basis for a Wiretap Act claim, as the MCC alleges that all websites upon which Google serves ads consent to the placement of cookies by Google to accomplish that task. (See MCC ¶¶ 38-45 (describing how "[w]ebsite owners" allow "third-party companies such as Google to serve advertisements directly," which involve the placement of "third-party cookies on individuals' computers").)

Sussman v. Am. Broadcasting Cos., 186 F.3d 1200, 1202-03 (9th Cir. 1999) ("Under section 2511, 'the focus is not upon whether the interception itself violation another law; it is upon whether the purpose for the interception – its intended use – was criminal or tortious.'" (internal quotation omitted)). The instant lawsuit is one about allegedly illegal means – "the scheme to track the Plaintiffs' communications," (see MCC ¶ 195) – not an illegal purpose, and in such a circumstance, the Wiretap Act claim against Defendants must fail. Sussman, 186 F.3d at 1202-03 ("Where the purpose is not illegal or tortious, but the means are, the victims must seek redress elsewhere.").

L.C. v. Central Pa. Youth Ballet, 09-cv-2076, 2010 WL 2650640 (E.D. Pa. July 2, 2010), cited by Plaintiffs for the proposition that violating the Wiretap Act itself "operates to negate single party consent," (see Opp. Br. at 29), does not help Plaintiffs here. That case involved the video-taping and intentional distribution of an interview with a child – conducted by the ballet school where that child was a student – concerning the sexual assault of that child by another student at the school. See 2010 WL 2650640, at *2. Thus, the case is immediately problematic because it is unclear what the illegal interception was – it appears plaintiff L.C. agreed to a video-taped interview, but his parents did not. See id. at *2 (stating that defendants "proceeded to tape record an interview with L.C. concerning the . . . sexual assault without his parents' knowledge"). Even if L.C. can be read to support the (questionable) proposition that one-party consent is ineffective where an illegal interception of a communication occurs with the express purpose to later disclose the intercepted information, see id. at *3, such a rule would be inapplicable to this case, which is only about Defendants' "scheme" to track Plaintiffs' online communications. There are no facts pleaded to indicate that the interceptions in this case were

motivated by anything other than Defendants' desire to monetize Plaintiffs' internet usage, and thus the "criminal or tortious act" exception embodied in § 2511(2)(d) is inapplicable.

Plaintiffs also contend that § 2511(2)(d) does not protect Defendants here because Plaintiffs are minors, and thus "Defendants' consent is [i]rrelevant." (Opp. Br. at 29.) Specifically, Plaintiffs argue that "a minor's ability to contract and consent to an agreement has never been treated the same way as an adult." (See id.) This is undoubtedly true, and were this a contract case such an argument might have force. But this is not a contract case, and Plaintiffs have cited no authority for the proposition that the Wiretap Act's one-party consent regime depends on the age of the non-consenting party. Moreover, the sextet of Supreme Court decisions Plaintiffs cite 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, which is to determine whether Plaintiffs have stated plausible claims for the causes of action alleged. Their rhetoric notwithstanding, Plaintiffs have provided no legal basis to treat minors any differently than adults under the Wiretap Act.

The Wiretap Act claim must also fail because there are no allegations that Defendants intercepted "contents" of communications, as required by the Act. See Bartnicki, 200 F.3d at 115. In this regard, the Court agrees with the District of Delaware's cogent and persuasive Google Cookie decision, which holds that "contents" as defined in the Act consist of "information the user intended to communicate, such as the spoken words of a telephone call." 2013 WL 5582866, at *4 (citing United States v. Reed, 575 F.3d 900, 916 (9th Cir. 2009)). The converse of this rule is that "'personally identifiable information that is automatically generated by the communication' is not 'contents' for purposes of the Wiretap Act.'" See id. at *5

(quoting In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1062 (N.D. Cal. 2012)). The Ninth Circuit, in a recently published opinion, has expressly adopted a nearly identical standard. See Zynga, -- F.3d --, 2014 WL 1814029, at *7 ("we hold that under ECPA [the Wiretap Act], the terms 'contents' refers to the intended message conveyed by the communication, and does not include record information regarding the characteristics of the message that is generated in the course of the communication").

Nothing allegedly intercepted in this case can pass muster under this standard. Plaintiffs argue that IP addresses and URLs in particular contain or are themselves "contents" for purposes of the Wiretap Act. (See Opp. Br. at 30.) IP addresses – the unique numbers generated by an ISP to identify a device connected to the internet and "voluntarily turned over to direct" computer servers, United States v. Christie, 624 F.3d 558, 574 (3d Cir. 2010) – are simply not "contents" of a communication. See, e.g., In re Application of the U. S. for an Order Authorizing use of A Pen Register and Trap on [xxx] Internet Service Acc't, 396 F. Supp. 2d 45, 48 (D. Mass. 2005) ("If . . . the government is seeking only IP addresses of the web sites visited and nothing more, there is no problem."). Indeed, in the analogous Fourth Amendment context, email and IP addresses can be collected without a warrant because they "constitute addressing information and do not necessarily reveal any more about the underlying contents of communications than do phone numbers," which can be warrantlessly captured via pen registers. Zynga, 2014 WL 1814029, at *9 (quoting United States v. Forrester, 512 F.3d 500, 510 (9th Cir. 2008)); see also Christie, 624 F.3d at 574 ("[defendant] therefore had no reasonable expectation of privacy in his IP address and so cannot establish a Fourth Amendment violation."). Plaintiffs suggest no compelling reason (in fact, no reason at all) why Congress intended such "addressing

information" to be treated any differently for purposes of the Wiretap Act – neither does the text of the Act itself.

Instead, Plaintiffs' opposition brief focuses exclusively on the argument that URLs are contents.[13] The District of Delaware's Google Cookie decision, however, correctly highlights that "URLs [i.e., Uniform Resource Locators] do not change and are used to identify the physical location of documents" on servers connected to the internet. 2013 WL 5582866, at *5. This characterization is consistent with the MCC filed in this case, which describes one URL in particular as the "file path" for a specific video file contained in a folder on a web server owned or operated by Viacom. (See MCC § 78.) Characterized as such, the URLs in this case have less in common with "the spoken words of a telephone call," Google Cookie, 2013 WL 5582866, at *4, than they do with the telephone number dialed to initiate the call.

It thus rings hollow when Plaintiffs argue that the electronic video requests allegedly intercepted here are no different than the contents – i.e., the spoken words – of a telephone call to a video store. (See Opp. Br. at 34.) In the latter case, the video title spoken over the phone by a customer is the "substance, purport, or meaning" of the call itself, § 2510(8); in the former, the video title contained in the intercepted URL is the "physical" location of that video on the servers of the website generating the URL. Stated differently, words entered by a user into a Google search might themselves be considered contents if reproduced in a URL that is subsequently disclosed. See Zynga, 2014 WL 1814029, at *9 ("[u]nder some circumstances, a

[13] The Court cannot credit Plaintiffs' argument that Google intercepted communications containing birthdate and gender information. (See Opp. Br. 35.) Such an argument is foreclosed by the MCC itself, which expressly alleges that Viacom disclosed Plaintiffs' gender and age information, either directly or through the "rugrat" code. (See MCC ¶¶ 81, 98-99.) Indeed, the entirety of Plaintiffs' VPPA claim is premised on these very allegations. Plaintiffs cannot have it both ways – either Viacom told Google the age and sex of its users, or Google intercepted that information as Plaintiffs provided it to Viacom.

user's request to a search engine for specific information could constitute a communication such that divulging that search term to a third party" could result in disclosure of contents (citing In re Pen Register & Trap Application, 396 F. Supp. 2d at 49)). But the file path and video title information contained in the URLs allegedly intercepted in this case are static descriptions more akin to "identification and address information." See id. As such, the Wiretap Act claim must be dismissed for the additional reason that Plaintiffs fail to allege that Google intercepted the "contents" of an electronic communication at Viacom's behest.

E. The SCA Claim

Plaintiffs also allege that Google has violated the Stored Communications Act, 18 U.S.C. § 2701(a), which by operation of § 2707(a) creates a civil cause of action against: "whoever . . . intentionally accesses without authorization [or intentionally exceeds authorization to access] a facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is electronic storage in such system . . . ." (MCC §§ 165, 170.)[14] "Facility" is undefined, but "electronic communication service" is defined as any "service which provides to users thereof the ability to send or receive wire or electronic communications." § 2510(15).

Enacted as Title II of the Electronic Communications Privacy Act of 1986, the SCA was Congress's attempt to fill the possible gaps in Fourth Amendment protection created by the proliferation of third-party storage of electronic communications. Google Cookie, 2013 WL 5582866, at *6 ("because [copies of user e-mail created and retained by e-mail service providers

[14] Confusingly, the MCC states that the SCA claim is brought against Defendant Google only (see MCC at 40), yet later on the MCC also alleges that "Defendants" intentionally accessed their computers without authorization. (MCC § 165.) This latter allegation would imply that the SCA claim is in fact brought against Viacom as well. During briefing, however, all parties took the position that Plaintiffs intended to plead an SCA cause of action again Google only, and the Court will adopt that approach as well.

are] subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection" (quoting S. Rep No. 99-541 (1986), as reprinted in 1986 U.S.C.C.A.N. 3555, 3557)); see also Zynga, 2014 WL 1814029, at *4 (finding that the SCA "covers access to electronic information stored in third party computers"). The SCA thus protects individuals from the unauthorized acquisition or modification of certain of their communications while those communications are stored on someone else's computer. Garcia v. City of Laredo, Tex., 702 F.3d 788, 793 (5th Cir. 2012) ("the words of the statute were carefully chosen: '[T]he statute envisions a *provider* (the [internet service provider] 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*.'" (internal quotation omitted)), cert. denied, 133 S. Ct. 2859 (2013).

Under the Act's plain language, Plaintiffs' SCA claim would appear to be a nonstarter – this is a case where Defendants' alleged privacy violations stem from "cookies" placed on Plaintiffs' (or their parents') own computers, not any third-party device. (See generally MCC ¶¶ 72-82.) Recognizing this, Plaintiffs argue that their own personal computers should be considered "facilities" for purposes of the SCA, and that Google can plausibly be liable for its unauthorized access of information found there. (See Opp. Br. at 47.) But as Google correctly highlights, Plaintiffs' approach is problematic. (Google Reply Br. at 15-17.) First, it runs contrary to the vast majority of published and non-published decisions that have considered the issue. See Cousineau v. Microsoft Corp., No. 11-cv-1438, 2014 WL 1232593, at *7 (W.D. Wash. Mar. 25, 2014) (collecting cases); Morgan v. Preston, No. 13-cv-0403, 2013 WL 5963563, at *5 (M.D. Tenn. Nov. 7, 2013) ("the overwhelming body of law" supports the

conclusion that "an individual's personal computer is not a 'facility through which an electronic communication service is provided'"). Moreover, Plaintiffs' interpretation of the statute does violence to the SCA's user/provider dichotomy, see Garcia, 702 F.3d at 793, and would empower service providers to grant access to their users' personal computer's without such users' authorization. § 2701(c) ("the person or entity providing a wire or electronic communications service" can authorize access to a facility). Such a result would be illogical, and "[s]tatutes should be interpreted to avoid untenable distinctions and unreasonable results whenever possible." Am Tobacco Co. v. Patterson, 456 U.S. 63, 71 (1982).

Plaintiffs' interpretation of the SCA is untenable, and this Court – in agreement with the great majority of decisions to address the issue – finds that the SCA is not concerned with access of an individual's personal computer. The SCA claim against Google fails as a matter of law will be dismissed with prejudice.

F. The State Law Claims

Plaintiffs also fail to state a plausible claim under any of the state law theories alleged.[15]

1. The California Invasion of Privacy Act Claim (Count IV)

In its wiretapping provision, the California Invasion of Privacy Act makes it a crime to "willfully and without the consent of all parties to the communication" read or "learn the contents or meaning of any message, report, or communication while the same in transit or passing over any wire, line or cable . . . ." Cal. Penal Code § 631(a). Persons injured by a violation of Section 631(a) may bring a civil action for money damages or injunctive relief. See id. at § 637.2. The MCC alleges that Viacom "knowingly serv[ed] as the conduit through which

[15] Because the Court finds that Plaintiffs fail to plead a viable state law claim, the Court need not reach Viacom's argument that COPPA preempts those claims. (Viacom Mov. Br. at 32.)

Google placed its [cookies] in positions to intercept the content of Plaintiffs' Internet communications." (MCC ¶ 184.)

Defendants argue that because the MCC does not allege facts demonstrating the interception of "contents" for purposes of the Wiretap Act, it also cannot allege the interception of "contents or meaning" for CIPA purposes. (See Viacom Mov. Br. at 34; Google Mov. Br. at 23.) Both Defendants cite the Google Cookie decision for this proposition. See 2013 WL 5582866, at *5-6 (dismissing the Wiretap Act and CIPA claims because "plaintiffs' allegations do not demonstrate that Google intercepted any 'contents or meaning'"). Plaintiffs do not argue that this aspect of Google Cookie was wrong, nor do they contend that "contents or meaning" means something different under California law than "contents" does under federal law; instead, Plaintiffs argue the intercepted information "takes on new meaning [*i.e.*, becomes contents] when it is matched up with an individual child via a cookie's unique identifier." (Opp. Br. at 43.) This argument is misguided. Plaintiffs' wiretap claims – including the CIPA count – are predicated upon the interception of electronic communication, not its use. (See MCC ¶ 180). Thus, whatever Google or Viacom allegedly do with the Plaintiffs' online information after it is intercepted has no bearing upon the question of whether that information could properly be considered "contents" at the time of interception. And, as the Court has discussed in detail supra, URLs and IP addresses are not properly considered "contents" in the wiretapping context.

In short, courts read CIPA's wiretapping provision and the federal Wiretap Act to preclude identical conduct. See Google Cookie, 2013 WL 5582866, at *6; Hernandez v. Path, Inc., No. 12-cv-1515, 2012 WL 5194120, at *3, *5 (N.D. Cal. Oct. 19, 2012) (dismissing Wiretap Act and CIPA wiretapping claim because of plaintiff's failure to allege "interception"

for purposes of both statutes). Absent a compelling suggestion otherwise, this Court will do the same, and holds that CIPA claim must fail for the same reason that the Wiretap Act claim fails – there are no allegations that plausibly demonstrate the interception of the "contents or meaning" of Plaintiffs' communications. The CIPA claim will be dismissed with prejudice.

2. The New Jersey Computer Related Offenses Act Claim (Count V)

The New Jersey CROA claim will be dismissed as well. The 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. Sup. Ct. App. Div. June 28, 2012) ("This statute plainly requires a plaintiff to prove that he or she was 'damaged in business or property.'"). The MCC, however, is devoid of factual allegations regarding the "business or property" damage Plaintiffs have suffered as a result of Defendants collecting and monetizing their online information. Plaintiffs attempt to rescue their CROA claim by rehashing arguments made in the standing context – namely, that Defendants' use of cookies permitted the "acquisition and use of Plaintiffs' personal information for marketing purposes," which Plaintiffs equate to "property" damage. (See Opp. Br. at 53.) This contention fails for the same reason it failed vis-a-vis standing – just because Defendants can monetize Plaintiffs' internet usage does not mean Plaintiffs can do so as well. Without allegations demonstrating plausible damage to "business or property," Plaintiffs cannot state a claim for relief under the CROA, and Count V will be dismissed without prejudice. See Phillips, 515 F.3d at 236.

3. The Invasion of Privacy Claim (Count VI)

New Jersey recognizes the common law privacy tort of "intrusion upon seclusion."

Soliman v. Kushner Cos., Inc., 77 A.3d 1214, 1224 (N.J. Sup. Ct. App. Div. 2013) (quoting Hennessey v. Coastal Eagle Point Oil Co., 609 A.2d 11, 17 (N.J. 1992)). This tort imposes civil liability for invasion of privacy on "[o]ne 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). The privacy invasion "need not be physical"; indeed, it may arise from "some other form of investigation or examination" into an individual's "private concerns." See id. To succeed with a claim for intrusion upon seclusion, a plaintiff "must establish that he possessed a reasonable expectation of privacy" in the affairs or concerns intruded upon. See G.D. v. Kenny, 15 A.3d 300, 320 (N.J. 2011). Plaintiffs allege Defendants "took information from the privacy of the Plaintiffs' homes," thereby "intentionally intrud[ing] upon the Plaintiffs' solitude or seclusion . . . ." (MCC ¶ 195.)

The Court notes that the right to privacy created by the New Jersey constitution provides greater protection than the privacy right created by the federal Constitution. See State v. Reid, 945 A.2d 26, 32-34 (N.J. 2008) (stating that Article I, Paragraph 7 of the New Jersey constitution "provides more protection than federal law affords" and holding that under New Jersey law an individual has a protectable "privacy interest in the subscriber information he or she provides to an Internet service provider"). Moreover, New Jersey explicitly "recognizes a right to 'informational privacy,'" which encompasses "any information that is identifiable to an individual." State v. Reid, 914 A.2d 310, 314 (N.J. Sup. Ct. App. Div. 2007) (internal quotation omitted), aff'd as modified, 945 A.2d 26; Doe v. Poritz, 662 A.2d 367, 412 (N.J. 1995) ("We have found a constitutional right of privacy in many contexts, including the disclosure of

confidential or personal information."). This information includes both "assigned" information, like names and addresses, but also "generated" information, such as medical records and phone logs. See Reid, 914 A.2d at 314 ("[P]ersonal information will be defined as any information, no matter how trivial, that can be traced or linked to an identifiable individual."). Thus, it is not implausible that the MCC as constituted alleges facts demonstrating that for purposes of New Jersey law Plaintiffs had a reasonable expectation that certain aspects of their online identities remain private and that Defendants intruded upon those private concerns. While Defendants' use of cookies to acquire or intercept IP addresses and URLs is an insufficient basis upon which to predicate claims for the federal statutes alleged, it is entirely unclear from the parties' submissions that the same would be true under New Jersey law and its expansive view of individual privacy.

But the Court need not address that question at this juncture, because the MCC lacks allegations demonstrating that the alleged intrusion is "highly offensive" to a reasonable person, see Hennessey, 609 A.2d at 17, and thus the intrusion upon seclusion claim must fail for that reason. Paragraph 197, which states without more that Defendants' intrusion "would be highly offensive to a reasonable person" is, of course, entirely conclusory, and thus properly disregarded on a motion to dismiss for failure to state a claim. See Bistrian, 696 F.3d at 365. The MCC otherwise does not explain factually how Defendants' collection and monetization of online information would be offensive to the reasonable person, let alone exceedingly so. The intrusion upon seclusion claim will be dismissed; because it does not appear at this juncture that leave to amend would be futile, however, this dismissal will be without prejudice. See Phillips, 515 F.3d at 236.

4. The Unjust Enrichment Claim (Count VII)

As stated supra, New Jersey law does not recognize "unjust enrichment" as an independent cause of action sounding in tort. Goldsmith, 975 A.2d at 462-63. "The Restatement of Torts does not recognize unjust enrichment as an independent tort cause of action. Unjust enrichment is of course a familiar basis for imposition of liability in the law of contracts." Castro v. NYT Television, 851 A.2d 88, 98 (N.J. Sup. Ct. App. Div. 2004) (citing Restatement (Second) of Contracts § 345(d)). Indeed, "[t]he unjust enrichment doctrine requires that the plaintiff show 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 rights." VRG Corp. v. GKN Realty Corp., 641 A.2d 519, 554 (N.J. 1994); see also Mu Signa, Inc. v. Affine, Inc., No. 12-cv-1323 (FLW), 2013 WL 3772724, at *10 (D.N.J. July 17, 2013) (finding unjust enrichment only appropriate where, "if the true facts were known to plaintiff, he would have expected remuneration from defendant, at the time the benefit was conferred" (internal quotation omitted)).

This is not a quasi-contract case, and an unjust enrichment claim is inappropriate based upon the facts pleaded here. There are no allegations that Plaintiffs conferred any benefit on Defendants, nor are there any allegations that Plaintiffs expected or should have expected any sort of remuneration from them. Plaintiffs argue that the Defendants "received a direct benefit" from the information they collected from Plaintiffs. (Opp. Br. at 60.) But receipt of a benefit by a defendant and conferral of a benefit by a plaintiff are two different things, and it simply is not reasonable for a consumer – regardless of age – to use the internet without charge and expect compensation because a provider of online services has monetized that usage. The Court is

unaware of any legal authority that would find the relationship described in the MCC to be unjust in the contractual or quasi-contractual sense, and Plaintiffs do not suggest a cogent reason for the Court to find as such here. The common law "unjust enrichment" claim will be dismissed with prejudice.

IV. Conclusion

For the foregoing reasons, the Court will grant the motions to dismiss filed by Defendants Viacom Inc. and Google Inc. [Docket Entries 43 & 44.] The VPPA claim against Google is dismissed with prejudice, inasmuch as it is apparent that Plaintiffs cannot plead facts that would make Google a video tape service provider as that term is defined in the statute. The Wiretap Act, Stored Communication Act, California Invasion of Privacy Act, and state law unjust enrichment claims fail as a matter of law and will be dismissed with prejudice. The VPPA claim against Viacom, and the intrusion upon seclusion and New Jersey Computer Related Offenses Act claims against both Defendants, will be dismissed without prejudice, since it appears that the Plaintiffs could possibly plead facts sufficient to cure the defects in those claims. Plaintiffs will have forty-five (45) days to file an Amended Master Consolidated Class Action Complaint. An appropriate form of Order will be filed herewith.

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

Dated: July 2nd, 2014