IN THE

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 15-1441

In re Nickelodeon Consumer Privacy Litigation

Appeal from the United States District Court for the District of New Jersey
No. 2:12-cv-7829
The Honorable Stanley R. Chesler

BRIEF OF APPELLEE VIACOM INC.

Jeremy Feigelson
David A. O'Neil
Christopher S. Ford
DEBEVOISE & PLIMPTON LLP
919 Third Avenue
New York, N.Y. 10036

Stephen M. Orlofsky
BLANK ROME LLP
301 Carnegie Center
Princeton, N.J. 08540

Counsel for Appellee Viacom Inc.

CORPORATE DISCLOSURE STATEMENT

Viacom Inc. ("Viacom") is a non-governmental corporate party that has no parent corporation. No publicly held corporation owns 10% or more of Viacom's stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

STATEMENT OF THE ISSUES PRESENTED FOR REVIEW

1. Do Appellants have standing under Article III of the Constitution, given that their claims are not supported by any allegation of actual damages or real-world harm?

2. Did the District Court correctly dismiss Appellants' claim under the Video Privacy Protection Act ("VPPA"), given that VPPA prohibits the knowing disclosure of information that "identifies a person" but Appellants alleged only that Viacom disclosed anonymous information?

3. Did the District Court correctly dismiss Appellants' claim under the Electronic Communications Privacy Act ("ECPA"), given that: (*i*) ECPA is a one-party consent statute and Viacom was a consenting party to every alleged communication; and, independently, (*ii*) ECPA applies solely to the "contents" of communications, and the alleged disclosures consisted not of any contents, but simply of the webpage addresses visited by Appellants?

4. Did the District Court correctly dismiss Appellants' state-law claims under the California Invasion of Privacy Act ("CIPA"), the New Jersey Computer Related Offenses Act ("NJCROA"), and the common law of intrusion upon seclusion, given that: (*i*) Appellants have not stated a federal claim; (*ii*) the federal Children's Online Privacy Protection Act ("COPPA") preempts the

state-law claims; and (*iii*) on the merits, Appellants failed to state a claim under any of their state-law theories?

STATEMENT OF RELATED CASES AND PROCEEDINGS

No cases currently pending before this or any other Court are directly related to this case. *In re Google Cookie Placement Consumer Privacy Litigation*, No. 13-4300 ("*Google Cookie*"), currently pending before the Third Circuit, raises similar questions of law regarding: (1) Article III standing and (2) ECPA.

STATEMENT OF PROCEEDINGS BELOW

On October 23, 2013, Appellants filed their first consolidated complaint in this multi-district litigation. (App'x at 59.) That complaint asserted causes of action under three federal statutes: VPPA, ECPA and (as to Google only) the Stored Communications Act ("SCA"). The complaint also asserted causes of action under two state statutes, CIPA and NJCROA, and two common-law theories, unjust enrichment and intrusion upon seclusion.

On January 15, 2014, Viacom and Google each moved to dismiss all of Appellants' claims. The motions were based on Appellants' failure to state a claim, under Fed. R. Civ. P. 12(b)(6), and their lack of Article III standing, under Fed. R. Civ. P. 12(b)(1).

On July 2, 2014, the District Court (Hon. Stanley R. Chesler) issued a 39-page Opinion and Order dismissing the entire complaint. The District Court dismissed the VPPA claim as to Viacom without prejudice and as to Google with prejudice; the ECPA claim as to both defendants with prejudice; the SCA claim against Google with prejudice; the CIPA and unjust enrichment claims as to both defendants with prejudice; and the NJCROA and intrusion upon seclusion claims as to both defendants without prejudice. (App'x at 6.) The District Court upheld Appellants' standing under Article III. (App'x at 9.)

Appellants filed an amended consolidated complaint on September 11, 2014. The purpose of that amended complaint was to re-plead each of the claims that the District Court had dismissed without prejudice by attempting to supply the allegations that the District Court had concluded were missing or insufficient. On October 14, 2014, Viacom and Google again each moved to dismiss. On January 20, 2015, the District Court issued an 11-page Opinion and Order concluding that Appellants' complaint, even as revised, failed to state a claim and therefore dismissing all remaining claims with prejudice. (App'x at 47.)

STANDARD OF REVIEW

Appellants appeal from the two opinions and orders granting Viacom's and Google's motions to dismiss under Rule 12(b)(6). They do not challenge the District Court's dismissal of the unjust enrichment claim, but challenge the dismissal of all their other theories. Those rulings are reviewed *de novo*. *Balletine v. United States*, 486 F.3d 806, 808 (3d Cir. 2007).

ALLEGATIONS OF THE COMPLAINTS

Viacom operates the Nickelodeon television networks and associated websites such as Nick.com. (App'x at 59.) These free, advertising-supported websites feature popular productions like the cartoon series "SpongeBob SquarePants." (App'x at 91.) Appellants allege that when a user watches one of these productions, Viacom provides Google (which facilitates the delivery of

advertising) with an anonymous number string associated with the viewing session. The number string is called a universal unique identifier, or UUID, and is contained in a small text file called a cookie that resides on the user's computer. (App'x at 82–83.) Appellants also allege that Viacom permitted Google to place its own third-party cookie on users' computers, which contained another UUID linked to Google's DoubleClick advertising service. (App'x at 78.)

Nowhere in any of their pleadings do Appellants allege that Viacom ever learned their real names or any other details that actually identify them. Viacom's websites permitted users to register by creating a username and providing their age and gender, but users were instructed not to provide their real names or other contact details. (App'x at 81–82.) Appellants allege only that Viacom took the anonymous information supplied by registered users, encoded the age and gender data into a so-called "Rugrat" value, and stored their usernames and the "Rugrat" value in Viacom's first-party cookie. (App'x at 82.) According to Appellants, Viacom disclosed the "Rugrat" value to Google, along with the website addresses of each Viacom webpage that Appellants visited. (App'x at 82–83.)

SUMMARY OF ARGUMENT

Despite the bulk of their pleadings, all of Appellants' legal theories rest entirely on the handful of factual allegations summarized above. Those allegations do not state a claim for the following reasons:

First, Appellants lack standing because they have not alleged any injury-in-fact, whether suffered in the form of a financial loss or any other sort of harm. At most, Appellants have argued that Viacom used anonymous data about their Internet activity to facilitate the delivery of the very advertising that makes Viacom's websites available for free to them and the rest of the public. That is not the necessary injury-in-fact required for standing under Article III, even accepting as true the conclusory allegation that personally identifying information was disclosed. Under this Circuit's clear precedent, asserting that the words of a statute like VPPA are violated does not establish standing unless the assertion is supported by concrete allegations of real-world, actual injury.

Second, the District Court correctly held that the anonymous information transmitted by Viacom, "without more," is not within the scope of VPPA because the statute prohibits only disclosures that the discloser knows will identify a specific individual as having watched a particular video. (App'x at 21–22.) Appellants failed to plead facts showing that they were identified by the

information collected by Viacom, much less that Viacom knowingly disclosed their identities to Google.

Appellants assert instead that the anonymous UUID in a cookie "identifies a person" under VPPA – a theory at odds with the statutory language, the statute's legislative history and purpose, and the views of nearly every court to consider the issue. Anonymous identifiers cannot fit within VPPA's plain-English definition of information for which disclosure is actionable and do not trigger the privacy concerns that led to VPPA's enactment. Appellants did not and could not allege that Viacom ever collected their names or any other information about their real-world identities or that it knowingly disclosed such details to Google. Instead, they speculated that Google had the ability to combine the anonymous UUID with other information Google collected on its own – about Appellants' parents – to deduce Appellants' identities. The District Court correctly held that failed to state a VPPA claim.

Third, the District Court correctly held that Appellants' allegations under ECPA fail as a matter of law:

- ECPA is a one-party consent statute. There can be no statutory violation where, as here, one of the parties to a communication consents to the alleged interception. According to Appellants' own allegations, Viacom was a party to every communication at issue and

consented to every interception. Appellants' counter-argument, that interception is itself a tortious act that invalidates Viacom's consent, has been consistently rejected by courts for over a decade, and Appellants' theory that their age invalidates Viacom's consent has no basis in the statute, caselaw, or common sense.

- ECPA applies only to the "contents" of communications, not to the static webpage addresses (URLs) that Appellants pled as the basis of their ECPA claim. Those URLs serve the same function as a physical address or a telephone number: They identify where a computer can find a website on the Internet, but they do not contain, or communicate the substance of, any communication between the user and the website.

In the absence of well-pled allegations of fact showing a violation of VPPA or ECPA, Appellants (and their supporting amicus) substitute a pair of sweeping policy arguments: (*i*) that children deserve special legal protection, and (*ii*) that Google deserves special scrutiny due to its prominence in the Internet ecosystem and its purported ability, alleged in purely conclusory terms, to connect anonymous data to Internet users' real-world identities. Policy arguments cannot salvage pleading failures. Appellants have not pled any knowing disclosure by Viacom to

Google of statutorily protected information under VPPA, or any unauthorized interception under ECPA.

Fourth, the District Court correctly dismissed the state-law claims. This Court need not and should not reach those claims, given the absence of any federal claim and given the preemption provisions of COPPA, which establishes a uniform federal standard for the protection of children's privacy online. If this Court does consider the substantive adequacy of Appellants' pleading under state law, it should affirm the District Court's dismissals. The CIPA claim fails because Appellants do not plead that their communications have been disclosed. The NJROA claim fails because there is no allegation of harm to business or property, as New Jersey law requires. The intrusion upon seclusion claim requires allegations of "highly offensive" conduct but is pled and argued based on nothing more than the use of cookies in the ordinary operation of the Internet, which is not "highly offensive" as a matter of law.

ARGUMENT

I. Appellants' Federal Claims Were Properly Dismissed.

Appellants have not alleged "enough facts to state a claim to relief that is plausible on its face," as they must to survive a motion to dismiss under Fed. R. Civ. P. 12(b)(6). *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). For purposes of such a motion, well-pled factual allegations must be accepted as true,

but the Court need not credit "legal conclusion[s] couched as . . . factual allegation[s]." *Baraka v. McGreevey*, 481 F.3d 187, 195 (3d Cir. 2007); *see also Fowler v. UPMC Shadyside*, 578 F.3d 203, 210–11 (3d Cir. 2009). Appellants' pleadings are long on conclusions, suppositions, and assertions of theory and policy, but short on specific facts. That is fatal to their case.

A. Appellants Lack Standing Under Article III.

This Court has "an independent obligation to ensure" that Appellants have Article III standing, *Wilson v. Sec. Pa. Dep't of Corr.*, 782 F.3d 110, 114 (3d Cir. 2015), and it may affirm on any ground supported by the record, *Iwanicki v. Pa. Dep't of Corrections*, 582 F. App'x 75, 78 (3d Cir. 2014). Thus, although the District Court held that Appellants had standing – despite expressing "doubts" over their real-world injury (App'x at 13), standing is a threshold issue properly considered on this appeal.

Appellants allege no injury-in-fact. They plead only that a statute was violated. (App'x at 12–13.) This is insufficient under Article III.

"[T]he proper analysis of standing focuses on whether the plaintiff suffered an actual injury, ***not on whether a statute was violated***." *Doe v. Nat'l Bd. of Med. Exam'rs*, 199 F.3d 146, 153 (3d Cir. 1999) (emphasis added) (on a statutory claim, identifying an individual by name as disabled on test scores resulted in an actual injury for Article III purposes); *see also Danvers v. Ford Motor Co.*, 432 F.3d 286,

290–91 (3d Cir. 2005) (Alito, J.) (abstract, hypothetical harms are insufficient to satisfy Article III's requirement of a "concrete and particularized" injury-in-fact); *Fair Housing Council v. Main Line Times*, 141 F.3d 439, 443–44 (3d Cir. 1998) (holding that "a violation of the [Fair Housing] Act does not automatically confer standing on any plaintiff").

An alleged violation of a statutory prohibition thus is not enough without allegations that the violation caused an actual injury. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 578 (1992) (Congress may "elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law" but may not "abandon[] the requirement that the party seeking review must himself have suffered an injury"); *In re Horizon Healthcare Servs. Inc. Data Breach Litig.*, No. 13-7418, 2015 WL 1472483, at *5–6 (D.N.J. Mar. 31, 2015) (granting motion to dismiss plaintiffs' federal statutory claims after a data breach, where plaintiffs "do not allege any specific harm . . . and therefore may not rest on mere violations of statutory and common law rights to maintain standing" and declining to find standing where any injury would only result from a "hypothetical string of events"). Congress may define certain injuries as actionable by statute, *see generally Warth v. Seldin*, 422 U.S. 490, 500 (1975) (holding that the "injury required by Art. III may exist solely by virtue of statutes creating legal rights"

(internal quotation marks omitted)), but an actual injury – in addition to a violation of statutory language – still must exist for Article III's requirements to be met.

Here, Appellants have attempted to plead, at best, that the prohibitions set forth in VPPA and ECPA were violated, but they have not articulated an actual injury that resulted from the alleged violations. Instead, they offer hypotheticals about the potential economic value of their individual data (App'x at 71-74), but they do not allege they have ever attempted to use, let alone monetize, that data or that their ability to do so was in any way diminished. *See, e.g.*, *Whitmore v. Arkansas*, 495 U.S. 149, 155 (1990) (holding that a plaintiff must identify an injury-in-fact that is "distinct and palpable" as opposed to "merely abstract"); *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3rd Cir. 2011) (affirming dismissal in an invasion of privacy case because "allegations of hypothetical, future injury do not establish standing under Article III").

Other federal courts have recognized that allegations of technical statutory violations, just like those alleged here, do not demonstrate the injury-in-fact that Article III requires. *See Sterk v. Best Buy Stores, L.P.*, No. 11-C-1894, 2012 WL 5197901, at *5–7 (N.D. Ill. Oct. 17, 2012) (no standing for an alleged VPPA violation without allegation of concrete harm); *LaCourt v. Specific Media, Inc.*, No. SACV 10-1256, 2011 WL 1661532, at *1 (C.D. Cal. Apr. 28, 2011) (no

standing for cookie-based data collection absent real-world injury). This Court should do the same.[1]

B. The District Court Properly Dismissed Appellants' VPPA Claim Because Viacom Did Not Knowingly Disclose Information That Identified Appellants.

VPPA was enacted in response to a specific privacy violation: In 1987, a reporter was investigating then-Supreme Court nominee Judge Robert Bork in connection with his confirmation hearing. To pry into Judge Bork's video tape viewing habits, he persuaded a clerk at Judge Bork's local video store to hand over a list of the video tapes Judge Bork had rented. S. Rep. No. 100-599, at 5, *reprinted in* 1988 U.S.C.C.A.N. 4342-1, 4342-5 ("VPPA Senate Report").

Congress found that to be an "outrageous invasion of privacy." 134 Cong. Rec. 16,314 (daily ed. Oct. 13, 1985) (statement of Sen. Charles E. Grassley). It enacted VPPA to outlaw such conduct by prohibiting:

- video tape service providers from "***knowingly***" disclosing
- information they have collected

[1] The Supreme Court recently granted *certiorari* to resolve, during the October 2015 Term, a similar standing question under the Fair Credit Reporting Act. *Spokeo v. Robins*, 742 F.3d 409 (9th Cir. 2014), *cert. granted*, No. 13-1339, 2015 WL 1879778 (U.S. Apr. 27, 2015). A similar standing issue is before this Court in *In re Google Cookie Placement Consumer Privacy Litigation*, No. 13-4300 (3d Cir.).

- when that information "***identifies a person*** as having requested or obtained specific video materials" ("PII").

18 U.S.C. §§ 2710(a)(3) & (b) (emphasis added). *See also* VPPA Senate Report, 1988 U.S.C.C.A.N. at 4342-1 (VPPA only applies when the disclosed information "***identifies a particular person*** as having engaged in a specific transaction" (emphasis added)). According to the accompanying Senate Report, VPPA embodies the "central principle…that information collected for one purpose may not be used for a different purpose." VPPA Senate Report, 1988 U.S.C.C.A.N. at 4342-8.

The District Court twice held that Appellants had not alleged facts that establish the required elements of a VPPA claim. It dismissed their original VPPA claim, gave them every opportunity to cure the defects by amendment, and then concluded the amended pleading was equally lacking. The District Court correctly held that VPPA requires a knowing disclosure of information collected by a video tape service provider that, "***without more***, itself link[s] an ***actual person*** to actual video materials." (App'x at 24 (emphasis added).) It found no indication, in the text of the statute, the legislative history or elsewhere, that a VPPA claim can be stated based on Appellants' theory: that the statute prohibits a disclosure of "anonymous information" which, after investigation and coupled with still other information collected from other sources, may "lead to the identification of a specific person's video viewing habits." (App'x at 25.) Anonymous information,

however, is all the Complaint alleges was disclosed here. (*See, e.g.*, App'x at 215–19.)

Not only is Appellants' interpretation of VPPA overbroad, but the District Court also noted that the Complaint failed as being "entirely theoretical." (App'x at 52.) It correctly pointed out that

> the [Complaint] 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***.

(*Id*. (emphasis added).)

The District Court's holding about the specific factual allegations required to state a VPPA claim flows directly from VPPA's plain language: The statute prohibits a disclosure, made knowingly by the disclosing party, of information collected by that party, which "***identifies a person***." 18 U.S.C. § 2710(a)(3) (emphasis added). It does not prohibit the disclosure of cookies or similar coded information, used for decades to facilitate the operation of the Internet, that theoretically could be used by the recipient to identify the location of a connected computer.

Appellants concede, as they must, that Viacom did not "knowingly" disclose to Google any information that identifies any specific "person." (Appellant's Brief at 23.) Instead, the focus of the alleged disclosure is anonymous data strings purportedly combined by Google with information Google separately has

collected. (App'x at 141, ¶ 107.) Viacom, however, is not alleged to have had access to – or even known about – that separate information, or how Google might combine it with the only disclosure Viacom is alleged to have made: a UUID contained in a cookie and an anonymous "Rugrat" code, neither of which identify a person. (App'x at 219; Appellant's Brief at 7.) The Rugrat code contained encoded age and gender data that could not be understood by Google – not personally identifiable details. (App'x at 220–23, 225; Appellant's Brief at 7.)

That does not state a claim: (1) Viacom cannot "knowingly" disclose the identities of Appellants when it is not even alleged to have collected those identities or to know what Google can do with Viacom's data; (2) anonymous information does not fit within VPPA's definition of PII because it does not itself "identify a person;" and (3) the purported ability of Google to use anonymous information to identify Appellants is both (*i*) pure speculation and (*ii*) contradicted by the only specific facts alleged in the Complaint. No court has held that the type of anonymous information collected and disclosed by Viacom is within the scope of VPPA.

1. There Was No "Knowing" Disclosure Of VPPA PII By Viacom.

Appellants do not plead facts that, even if accepted as true, allege their actual identities were (*i*) collected by Viacom and (*ii*) knowingly disclosed by Viacom to Google. Without both, Viacom cannot have violated VPPA.

Appellants do not, and truthfully could not, even allege that Viacom ever knew their actual identities. (*See, e.g.*, App'x at 215–19.) The purpose of VPPA is to prevent a video tape service provider from disclosing a particular, known person's identity and what videos they have watched. Viacom, however, is never alleged to collect the type of information at which VPPA is directed, (App'x at 133), and its only alleged disclosures are of (*i*) an automatically-generated anonymous UUID, embedded in a cookie placed on the computer used to access Viacom's website and (*ii*) the "Rugrat" code that Appellants allege Viacom, but not Google, understood to refer to age and gender.

Multiple courts considering the identical question have concluded that information falling so far short of identifying a "person" is not PII for purposes of VPPA. *See, e.g.*, *Eichenberger v. ESPN*, No. 2:14-cv-463, Judgment by Court, Dkt. 47 (W.D. Wa. May 7, 2015) ("In light of the VPPA's text and legislative history, 'personally identifiable information' under the VPPA means information that identifies a specific individual and is not merely an anonymous identifier.") (appeal pending); *Locklear v. Dow Jones & Co.*, No. 14-cv-744, 2015 WL 1730068, at *6 (N.D. Ga. Jan. 23, 2015) ("The Court concludes that [the] Roku serial number, '***without more***,' is not akin to identifying a particular person and, therefore, is not PII." (emphasis added)) (appeal pending); *Ellis v. Cartoon Network*, No. 1:14-cv-484, 2014 WL 5023535, at *3 (N.D. Ga. Nov. 6, 2014)

("The Android ID is a randomly generated number that is unique to each user and device. It is not, however, akin to a name. ***Without more***, an Android ID does not identify a specific person." (emphasis added)) (appeal pending). The "more" was fatally lacking in those cases and is lacking here.

VPPA also imposes a separate requirement that the prohibited disclosure of PII must have been done "knowingly." 18 U.S.C. § 2710(b)(1). By definition, Viacom cannot "knowingly" disclose that which it does not know: the identity of the "person" to whom the anonymous codes are assigned. Nor can it "knowingly" disclose PII for purposes of VPPA when it is not alleged to know the information with which the anonymous coded information will be combined.

2. VPPA Prohibits Knowing Disclosures of PII, Not The Use Of Anonymous Information By Recipients.

Appellants never directly challenge the foregoing common sense, plain meaning approach to VPPA. (App'x at 153.) Instead, their arguments turn entirely on speculation that an allegedly omniscient and omnipotent Google somehow can discover a person's identity, even when Viacom does not know it and did not disclose it. (App'x at 131, ¶ 79 (referring generally to Google's "ubiquitous" presence on the Internet); *id.* ¶¶ 131–138 (providing a lengthy list of data collected by Google in various other contexts, none of which is alleged, in anything other than purely conclusory terms, to be tied to the anonymous data allegedly shared by Viacom).)

Appellants were obligated to plead that they were identified by the information that ***Viacom*** disclosed, not that they might be identified based on what they speculate ***Google*** might be able to do with other information not collected by Viacom. They have twice failed to do so and the rank speculation they offer is completely contradicted by the few specific facts in their Complaint, which incorporate by reference Google's Privacy Policy. (App'x at 225–26.) That policy stated, during the time period of Appellants' alleged activity, that Google "***will not*** combine DoubleClick cookie information with personally identifiable information unless [Google has the user's] opt-in consent." (App'x at 135–36 (emphasis added).)

Moreover, Appellants never allege that they themselves have Google accounts or are even Google users. (App'x at 131–38, ¶¶ 78–99.)[2] The best they can claim is that it is their parents, not Appellants themselves, about whom Google had collected other information, as a result of those adults having created and used

[2] As noted in Viacom's argument below (D.N.J. Docket No. 77-1 at 5 n.1), Google's policy excludes users under the age of 13. *See* "Age Requirements on Google Accounts," *https://support.google.com/accounts/answer/1350409?hl=en* ("Below are the minimum age requirements to own a Google Account: United States: 13 or older"). This Court may properly consider publicly available materials relating to Google's services, as they are integral to Plaintiffs' factual allegations. *See In re Burlington Coat Factory Sec. Litig.*, 114 F.3d 1410, 1426 (3d Cir. 1997) (a court considering a Rule 12(b)(6) motion may consider documents that, although not attached to the complaint, are integral to it).

Google accounts. *See* Appellants' Brief at 22 n.6. This only underscores that the purported UUID disclosure by Viacom fails to identify "a particular person," as the statute requires. VPPA Senate Report, 1988 U.S.C.C.A.N. at 4342-1. The UUID is assigned to a computer. It is not assigned to any one of the unknown number of people who used that computer. *See* Appellants' Brief at 6–7. Appellants acknowledge that the same anonymous UUID would be disclosed by Viacom regardless of who uses the computer in question – Appellants, their parents or third parties. *Id.* at 22 n.6. That level of generality is not within the scope of the key statutory words: "identifies a person." 18 U.S.C. § 2710(a)(3).

Appellants' argument also is completely inconsistent with VPPA's requirement that disclosures of PII must be both knowing and made by the video tape service provider, independent of any action then taken by the alleged recipient. Under Appellants' approach, A's disclosure of anonymous information to B would satisfy the "knowing" element based solely on what B might be able to deduce from the information.

That makes no sense: The focus of the statute is exclusively on the conduct of the disclosing party. The plain language prohibits a disclosure, by a video tape service provider, of information that the provider knows "identifies a person," not information that (as Appellants would, in substance, rewrite the law) 'can be used

by a recipient, along with other information in the recipient's sole possession, to identify a person.'

In an analogous privacy context, this Court previously has interpreted "information that identifies" a person to include only those specifically identified by the information at issue and to exclude others who might be identified were the information to be used as a starting point to track them down. *See Pichler v. UNITE*, 542 F.3d 380 (3d Cir. 2008) (individuals not specifically identified in motor vehicle records had no standing to sue under the Drivers Privacy Protection Act, ("DPPA"), 18 U.S.C. § 2721 *et seq.*, which prohibits the obtaining, use ordisclosure from motor vehicle records of "information that identifies an individual" or person, *id*. § 2725(3)).

Pichler held that the plain language of DPPA applied only to the actual person whose information was directly obtained – *i.e.*, the husbands who were the registered owners of the cars. Allowing spouses to sue because they could be connected to their husbands by further due diligence read the statute "too broadly" and would result in an "unwarranted extension." 542 F.3d at 391.

The same reasoning applies here. VPPA is triggered by "knowing" disclosures of information identifying a person that a video tape service provider itself collects and discloses. It does not turn on how others may use the disclosed information to continue the identification process. *Pichler* stands for the

proposition that a connect-the-dots approach – making ***Viacom*** liable for what ***Google*** might be able to deduce – is beyond the scope of the statute.

Congress' reference in VPPA to information that "identifies a person" must be given its plain meaning. *See Hartford Underwriters Ins. Co. v. Union Planters Bank, N.A.*, 530 U.S. 1, 6 (2000) ("[W]hen the statute's language is plain, the sole function of the courts—at least where the disposition required by the text is not absurd—is to enforce it according to its terms." (internal quotation marks omitted)). The importance of construing a statute according to its plain terms is especially significant where, as here, litigants seek dramatically to expand its scope to cover conduct that does not follow from the statutory text or any purpose identified in the legislative history. Appellants' expansive reading would be potentially crippling and produce absurd results: VPPA provides for statutory damages of $2,500 per violation, a figure that quickly becomes astronomical when multiplied at Internet scale. That result is particularly absurd given that Appellants are now using VPPA to condemn the use of cookies, which for years have been accepted by courts as a staple of Internet commerce. *See infra* pp. 40 – 43. Moreover, their theory would sweep within VPPA IP addresses, a whole range of device identifiers and all sorts of information that allows the Internet to function smoothly by directing communications between users and websites. *See Griffin v. Oceanic Contractors, Inc.*, 458 U.S. 564, 575 (1982) ("[I]nterpretations of a statute

which would produce absurd results are to be avoided if alternative interpretations consistent with the legislative purpose are available."); *see also Clinton v. City of New York*, 524 U.S. 417, 429 (1998) (rejecting interpretation of statute that "would produce an absurd and unjust result which Congress could not have intended" (citing *Griffin*)).

Appellants nonetheless urge this Court to expand VPPA because ***other*** statutes use different, broader definitions of PII. *See* Appellants' Brief at 18–26. VPPA itself, however, uses a clear, plain-meaning definition and every one of the statutes Appellants cite was passed before Congress most recently amended VPPA, in 2012. Video Privacy Protection Act Amendments Act of 2012, H.R. 6671, 112th Cong. (2012). Had Congress wished to modify VPPA's definition of PII to conform it to other statutory regimes, it easily could have done so. It did not.

Because, under VPPA, PII has a plain legal meaning, one that the district court interpreted and correctly applied, whether a UUID is PII does not require findings of fact by a jury. *See, e.g.*, *Drakes v. Zimski*, 240 F.3d 246 (3d Cir. 2001) (interpreting a statutory definition is "a question of law" that can be decided by the court). Appellants' argument to the contrary, Appellants' Brief at 26, is simply wrong.

The extent to which Appellants' VPPA arguments are based on policy, rather than a plain reading of VPPA's express language, is epitomized by the

submission of *amicus* the Electronic Privacy Information Center ("EPIC"). EPIC argues for a definition of PII under VPPA that includes "deductive disclosure" – *i.e.*, a regime where it is actionable for A to disclose anonymous information about a person to B, who somehow deduces the person's identity. *See* EPIC Amicus Brief at 5. That approach cannot be reconciled with VPPA's exclusive focus on what the video tape service provider itself knowingly discloses. It runs counter to virtually every court decision analyzing VPPA to date and improperly would rewrite the plain terms of VPPA. *See In re Hulu Privacy Litig.*, No. C-11-03764 LB, 2014 WL 1724344, at *12 (N.D. Cal. 2014) (rejecting argument that broader definition of PII under COPPA should apply in case brought under VPPA).

3. No Court Has Held That The Anonymous Information Viacom Allegedly Disclosed Is PII For VPPA Purposes.

None of the cases cited by Appellants have adopted the theory that a VPPA violation can be established based on speculation about the ability of a person, other than the disclosing party, to connect the dots from a UUID or other anonymous information to identify a person. *Cf.* Appellants' Brief, at 19–20. In fact, they explicitly reject it. *See Locklear*, 2015 WL 1730068, at *6 (plaintiff alleged specifically that the third party who received a UUID "was able to identify her and attribute her video records" by using "data linked to a Roku serial number"); *Ellis*, 2014 WL 5023535, at *1 (plaintiff alleged that the receiving party "was able to reverse engineer the consumers' identities using the information

previously collected from other sources"). In both *Ellis* and *Locklear*, the district courts dismissed plaintiffs' VPPA claims at the pleading stage because the information allegedly disclosed did not, without more, identify a person.

The only two district courts that have allowed a VPPA claim to go forward based on the disclosure of a numeric identifier did so on factual allegations wholly unlike this case. In *In re Hulu,* users of the online video service Hulu voluntarily could link their Hulu accounts to their Facebook accounts and grant Hulu access to their Facebook IDs. Those Facebook IDs contained real-world identifying information including the plaintiffs' Facebook user names, which they had provided to Facebook upon registration with that service. Therefore, the alleged disclosure by Hulu to Facebook of the Facebook IDs resulted in the inherent and immediate disclosure of the names of those users to Facebook. On those facts, the district court allowed the VPPA claim to go forward. *In re Hulu*, 2014 WL 1724344, at *14.[3]

Appellants, however, do not allege that ***they themselves*** signed up for one of Google's services – they do not allege they even had Google accounts, which is the mechanism by which Google purportedly connected the dots. Nor do they allege

[3] The *Hulu* court eventually granted summary judgment for Hulu on the basis that plaintiffs could not show Hulu had the requisite knowledge of Facebook's ability to connect the dots. *In re Hulu Privacy Litig.*, No. 11-cv-3764, 2015 WL 1503506, at *12 (N.D. Cal. Mar. 31, 2015).

that they ever provided Google with their names. Such basic pleading failures mean the Complaint lacks any allegation that the UUIDs identify Appellants. (App'x at 133.) The information Google purportedly collects about other people, *see* Appellants' Brief at 9, cannot substitute for specific facts about the Appellants in this case.

Yershov v. Gannett Satellite Info. Network, Inc., No. 14-13112, 2015 WL 2340752 (D. Mass. May 15, 2015), decided since Appellants filed their brief, is another case dismissing efforts to apply VPPA to circumstances it never was intended to cover. The district court held that Gannett's distribution of a free mobile application for Android phones did not give rise to a VPPA claim, because those who downloaded the application were not "subscribers" as VPPA requires.

The *Yershov* court opined, in *dicta*, that an anonymous identifier in an Android smartphone, when combined with GPS data, could be PII under VPPA. *Id.* at *8. That *dicta*, however, is neither controlling nor correct.

- The *Yershov* court expressly based its views on definitions of PII derived from other statutory contexts, not on the statutory text, history or purpose of VPPA. *Id.* at *5–6 (considering, for example, the definition of PII under ECPA).
- The *Yershov* court was persuaded that the Android ID could be VPPA PII because smartphones typically contain vast amounts of personal information,

which, as the Supreme Court concluded in a different context, meant they are protected from unreasonable searches and seizures under the Fourth Amendment. *Id*. (citing *Riley v. California*, 134 S. Ct. 2473 (2014)). That an anonymous identifier may be tied to such a device, which if accessed would contain identifying information, is no basis for ignoring the VPPA definition of PII. That definition requires the disclosure itself, not the device, to identify the individual. *See* pp. 15–16, *supra*.

- The *Yershov* court's observation that Social Security numbers (SSNs) or similar information can be personally identifying is not relevant to whether the anonymous data here qualifies as personal information under VPPA. The definition of PII, for purposes of VPPA, is specific and to be applied as written: It is information that identifies a person and connects that person to the titles of the videos they viewed. No such identification is alleged here: Viacom is not alleged either to have known the actual identities of its online viewers, or to have shared them with Google. Nor are any facts alleged that Google had the ability (as would the Social Security Administration with SSNs) to take Viacom's facially anonymous data and associate it with Appellants.
- The *Yershov* court essentially endorsed the connect-the-dots approach to defining VPPA PII that this Court rejected in *Pichler*.

For these reasons, the *dicta* in *Yershov* is at odds with the plain language of VPPA and this Court's holding in *Pichler*. The facts also are wholly distinguishable. Appellants allege the disclosure of a cookie-based UUID, which resides on a computer and can be deleted at the user's will. By contrast, the disclosure in *Yershov* was the combination of (*i*) the "Android ID" that is permanently assigned to a particular smartphone – a uniquely personal device, as contrasted with the shared family computers like the ones Appellants admit they used – and (*ii*) the user's exact GPS location. *Yershov*, 2015 WL 2340752, at *5. Appellants allege no comparable disclosure – nor could they, because cookie-based UUIDs do not behave like the Android ID, and Viacom never had access to Appellants' GPS locations.

* * *

Viacom's disclosure of an anonymous UUID and "Rugrat" code to Google was not a knowing disclosure of personally identifying information about Appellants to Google under VPPA. This Court should affirm the dismissal with prejudice of Appellants' VPPA claim as to Viacom.

C. The District Court Properly Dismissed Appellants' ECPA Claim.

1. Because ECPA Is A One-Party Consent Statute, Appellants Cannot State A Claim In Light Of Viacom's Consent.

ECPA is a one-party consent statute. There can be no violation of ECPA given that – as Appellants themselves have pled – Viacom placed its own cookie

on the user's computer, and Viacom likewise consented to Google placing a cookie as part of a different communication to which Viacom was also a party. (App'x at 82 ("Viacom provided Google with the online records . . . .").)

ECPA's civil liability provisions apply to any actor who "intercept[s], disclose[s], or intentionally use[s]" the contents of an electronic communication in a manner that violates the Act. 18 U.S.C. §§ 2511(1)(a), 2520(a). It exempts from liability, however, any "party to the communication" and further precludes liability "where one of the parties to the communication has given prior consent to such interception." 18 U.S.C. § 2511(2)(d). This exemption applies "unless such communication is intercepted for the purpose of committing any criminal or tortious act." *Id.*

The District Court held that Appellants' ECPA claim was fundamentally insufficient and dismissed it with prejudice in its first opinion. (App'x at 30.) It did so because Appellants both cannot overcome Viacom's consent, which removes any possibility of ECPA liability (App'x at 31), and because, as a matter of law, the URLs identified by Appellants in their pleadings are not "contents" under ECPA (App'x at 33). The District Court carefully considered every argument Appellants reiterate here, and correctly found each to be lacking.

Appellants acknowledge (*i*) that Viacom consented to the placement of both their own first-party cookie as well as Google's third-party cookie,ß and (*ii*) that

Viacom was a party to every alleged interception that they plead. (App'x at 78.) That completely invalidates their ECPA claim. Under established law going back over a decade to in *In re DoubleClick*, courts have unanimously rejected the argument that the placement of cookies violates ECPA. *See* 154 F. Supp. 2d 497 (S.D.N.Y. 2001). In that case, as now, plaintiffs attempted to bring a class action complaint on the theory that Google's placement of DoubleClick cookies violated ECPA. The district court rejected that attempt, holding the website operator's consent to Google's placement of those cookies was consent under ECPA that precluded plaintiffs' claims.

Appellants do not challenge that well-settled law but argue instead that, because they were minors at the time of the interception, Viacom's consent was somehow invalidated. *See* Appellants' Brief at 40–41. That makes no sense. Because ECPA does not require the consent of all parties, it cannot preclude party A from consenting because party B is a minor.

That should spell the end of Appellants' ECPA claim, but Appellants also argue that Viacom's acts fall within the narrow exemption for purposeful tortious acts. For two reasons, Appellants cannot establish the application of that exemption here.

First, Viacom's placement of cookies was – by Appellants' own admission – done to facilitate the delivery of advertising, not to commit a crime or a tort.

Viacom did not act with a tortious purpose. *See Chance v. Ave. A., Inc.*, 165 F. Supp. 2d 1153, 1163 (W.D. Wash. 2001) (ECPA "liability would only be possible if the tortious purpose were the primary motivation or determinative factor" behind the alleged actions, but it is "simply implausible that the entire business plan of one of the country's largest Internet media companies would be primarily motivated by a tortious or criminal purpose" (internal quotations and modifications omitted)).

Second, a long and consistent line of cases has held that ECPA's tortious act exemption only applies where there is "separate and independent tortious intent" falling outside of the interception itself. *Caro v. Weintraub*, 618 F.3d 94, 101 (2d Cir. 2010) (holding that a tortious act that "occurs through the act of interception itself . . . cannot satisfy [ECPA's] requirement of a ***separate and independent*** tortious intent" (emphasis added)); *see also Berk v. JP-Morgan Chase Bank, N.A.*, No. 11-2715, 2011 WL 6210674, at *3 (E.D. Pa. Dec. 13, 2011) (allegations of intrusion upon seclusion do not "satisfy the independent tortious intent requirement"). Appellants plead no separate tortious intent. Without the intent to commit an independent tortious act, the exemption does not apply.

Appellants cite one case in support of their argument that Viacom's interception, without more, can demonstrate an intent to commit a tortious act. *See L.C. v. Central Pa. Youth Ballet*, No. 1:09-cv-2076, 2010 WL 2650640, at *2 (M.D. Pa. July 2, 2010). That case involved exceptional facts involving plainly

offensive conduct: distribution of a recording of a student's description of a sexual assault. Moreover, to the extent that the case holds that such distribution is an independent "tortious act," that holding has never been followed by any other court. It has no application here.

There is no merit to Appellants' argument that Viacom could be liable for procuring Google to intercept communications (Appellants' Brief at 41), because ECPA does not permit a private cause of action for procurement. *See, e.g.*, *Kirch v. Embarq Mgmt. Co.*, 702 F.3d 1245, 1247 (10th Cir. 2012) (no civil liability for "procurement" under ECPA); *Peavy v. WFAA-TV, Inc.*, 221 F.3d 158, 169 (5th Cir. 2000) (same). Although "[t]he 1968 predecessor to ECPA imposed both criminal and civil liability for those who procured an interception," *Kirch*, 702 F.3d at 1247, when Congress enacted ECPA in 1986, Congress altered its civil provisions, "including deletion of the 'procures' clause." *Id.* "[T]his deletion was intended to change [Section 2520's] meaning." *Id.* Appellants therefore have no cause of action against Viacom based on any violation supposedly committed by Google.

Viacom's consent to the placement of the cookies at issue here defeats Appellants' ECPA claim. The District Court's opinion dismissing that claim with prejudice should be affirmed for this reason alone.

2. Webpage Addresses Are Not "Contents" Of Communications, As Is Required To State A Claim Under ECPA.

Viacom also did not disclose the "contents" of Plaintiffs' communication. 18 U.S.C. § 2511(1)(a)–(c), 2520(a). ECPA defines "contents" as "information concerning *the substance, purport or meaning* of [a] communication." *Id.* § 2510(8) (emphasis added). Absent the disclosure of contents, there can be no ECPA violation.

On appeal, Appellants now argue that Viacom disclosed "contents" to Google in the form of Appellants' age and gender, Appellants' Brief at 37. That goes beyond Appellants' actual allegations, which state only that Viacom disclosed the "Rugrat" code to Google without ever informing Google about the meaning of that code, which Viacom alone understood to relate to a user's age and gender. (App'x 140–41; id. 142 (Rugrat code alleged to contain age and gender information but not the user's name or any real-world identifying details).) This theory therefore should be disregarded. *See Twombly*, 550 U.S. at 570.

As to Appellants' original argument, the URL of a webpage is not the substance or meaning of a communication. Its disclosure therefore does not violate ECPA, as the District Court correctly held:

> 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. 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.

(App'x at 35 (internal citation omitted).)

Appellants concede that a URL "serves as the address" for a webpage, Appellants' Brief at 34, but argue that it also contains information. That a URL address may contain ***information*** does not mean it is equivalent to the ***substance*** of the communication facilitated by accessing a web page at that address. Appellants are wrong when they argue that, other than *In re Nickelodeon* and *Google Cookie*, "every federal court examining whether URLs contain contents under [ECPA] have ruled that they can or do." Appellants' Brief at 31. Indeed, as the court in *Google Cookie* noted, "[t]o date, no courts have characterized URLs as 'contents' for the purposes of [ECPA." 988 F. Supp. 2d 434, 444 (D. Del. Oct. 9, 2013). In *In re Zynga Privacy Litig.*, 750 F.3d 1098, 1108–09 (9th Cir. 2014), the Ninth Circuit held that standard URLs that identify websites are ***not*** contents for ECPA

purposes because those URLs include "only basic identification and address information." *Id.* at 1109. The Ninth Circuit distinguished such static URLs, which designate the address of a particular webpage – like every URL at issue in this case – from dynamically generated URLs used by search engines, which include a user's query and may therefore be deemed contents because such a URL "shows the specific search terms the user had communicated to Google." *Id.*

Here, the URLs Viacom allegedly disclosed to Google – like the "Penguins of Madagascar" URL that Appellants cite, Appellants' Brief at 35 – are not actionable under ECPA. A URL may contain the title of a video ("Skipper's Nightmare"), but it does not convey the substance, purport, or meaning of the video itself, nor a user's query – which are the only contents that ECPA theoretically might protect. *See In re § 2703(d) Order*, 787 F. Supp. 2d 430, 435–26 (E.D. Va. 2011) (holding that the spoken words of a telephone call are contents under ECPA, but a telephone number alone is not contents).

Appellants cannot evade this result by quoting snippets from the oral argument before this Court in the pending *Google Cookie* litigation. *See* Appellants' Brief at 30–31. The partial quote reflects, at most, Google's speculation that in some unknown and hypothetical circumstances – not those alleged here – URLs theoretically might constitute contents. *See generally Glick v. White Motor Co.*, 458 F.2d 1287, 1291 (3d Cir. 1972) ("The scope of judicial

admissions is restricted to matters of fact which otherwise would require evidentiary proof, and does not include counsel's statement of his conception of the legal theory of a case."). To state a claim, Appellants were required to plead facts demonstrating that, *in this case,* the "contents" of their communications were disclosed. They did not do so.

The other cases Appellants cite to support their URLs-as-contents theory do not even discuss URLs. *See* Appellants' Brief at 31; *Sams v. Yahoo*, No. CV-10-5897, 2011 WL 1884633 (N.D. Cal. May 18, 2011) (discussing user information including email addresses and IP addresses, nowhere mentioning URLs). Finally, whether URLs may be content under the Patriot Act or the Pen Register Act, *cf.* Appellants' Brief at 32–33, has no bearing on whether Congress intended to include them as content under ECPA. The District Court correctly dismissed Appellants' ECPA claim.

II. The District Court Properly Dismissed The State-Law Claims.

A. This Court Should Not Reach The Merits Of The State-Law Claims.

1. This Court Should Decline Jurisdiction Because Appellants Have Not Pled A Federal Claim.

Appellants fail to state a claim under any federal statute for the reasons stated above. For that reason, supplemental jurisdiction over Appellants' state-law claims should be declined, under the general rule that "[a]bsent extraordinary circumstances," state-law claims should be dismissed once the federal claims are

"no longer viable." *Kalick v. Northwest Airlines Corp.*, 372 F. App'x 317, 322 (3d Cir. 2010); *see also* 28 U.S.C. § 1367(c)(3). No such circumstances are presented by Appellants' efforts to transform the use of cookies into violations of law.

2. All The State-Law Claims Are Preempted By The Children's Online Privacy Protection Act.

COPPA establishes a uniform national standard for safeguarding children's privacy online. 15 U.S.C. § 6501 *et seq*. It contains an express preemption provision to ensure that website operators – whose sites are part of interstate commerce, capable of touching every corner of the country instantaneously – would not have to comply with a patchwork of 50 different state statutory and common law regimes. *See* 15 U.S.C. § 6502(d) (prohibiting enforcement of state laws that "impose any liability for commercial activities . . . in connection with an activity or action described in [COPPA] that is inconsistent with [COPPA's] treatment of those activities or actions"); *see also Fraley v. Facebook, Inc.*, 966 F. Supp. 2d 939 (N.D. Cal. 2013) (noting COPPA preemption issues relevant to a privacy class action settlement).

COPPA contains no private right of action, but, more importantly, for preemption purposes, nothing in it prohibits any of the activities on which Appellants base their state-law claims. Appellants nowhere allege facts that would indicate that Viacom (or Google) violated COPPA, nor could they. As a result, their state-law claims are expressly preempted by federal law and should be

dismissed for that reason alone. *See Kurns v. A.W. Chesterton, Inc.*, 620 F.3d 392, 395 (3d Cir. 2010), *aff'd*, 132 S. Ct. 1261 (2012) (applying doctrine of express preemption where a federal law contains "express language" providing for preemption).

B. The District Court Correctly Held That Appellants Have Failed To State Any State-Law Claims.

1. California Invasion of Privacy Act.

CIPA prohibits reading or learning "the *contents or meaning* of any message, report, or communication" while it is being transmitted. Cal. Penal Code § 631(a) (emphasis added). The URLs that Appellants allege Viacom disclosed to Google, however, are not the "contents" of any of Appellants' communications. *See supra* II.B.2. Just as no court has characterized URLs as contents for the purposes of ECPA, *see Google Cookie*, 988 F. Supp. 2d at 444, this Court should decline Appellants' invitation to expand CIPA to treat URLs as the contents of a communication. *See People v. Suite*, 161 Cal. Rptr. 825, 828 (Cal. Ct. App. 1980) (holding that CIPA does not apply to telephone numbers, as they are not the "contents" of a communication). The District Court properly found that Appellants did not state a claim under CIPA, and that holding should be affirmed.

2. New Jersey Computer Related Offenses Act.

Appellants' failure to allege any facts showing damage to their "business or property" precludes their asserting a claim under NJCROA, which plainly requires

such a showing of actual damages. N.J. Stat. Ann. § 2A:38A-3. Appellants try in vain to shoehorn a claim for unjust enrichment into the requirement of actual damages. Appellants' Brief at 47–49. By definition, however, unjust enrichment is never a measure of Appellants' own damage, and Appellants have no authority to support their novel theory that it should be. No court has ever accepted unjust enrichment as a measure of statutory damages under NJCROA.[4]

This Court previously has considered efforts to allege NJCROA claims, based solely on access to information (just as Appellants assert here), and concluded that such access is not enough to state a claim. *See P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504, 506 (3d Cir. 2005). In *P.C. Yonkers*, the plaintiff alleged "no proof of [defendant's] conduct other than access." *Id.* at 509. That was held insufficient, because NJCROA "require[s] proof of some activity vis-à-vis the information ***other than simply gaining access to it***." *Id.* (emphasis added); *see also PNC Mortg. v. Superior Mortg. Corp.*, No. 09-5084, 2014 WL 627995, at *4–6 (E.D. Pa. Feb. 27, 2012) (holding that allegations of "unauthorized" access were "simply not sufficient to sustain a claim" under NJCROA without a showing of harm). Appellants do not

[4] Appellants initially pled a standalone unjust enrichment claim, which was dismissed with prejudice, but Appellants do not raise that claim on appeal.

plead that any file residing on their computers was "taken" by Viacom. They therefore do not have a NJCROA claim. *See P.C. Yonkers*, 428 F.3d at 509.

3. Intrusion Upon Seclusion.

In New Jersey, the tort of intrusion upon seclusion has three distinct elements: (1) an intentional intrusion, (2) upon the seclusion of another, that was (3) highly offensive to a reasonable person. *See Hennessey v. Coastal Eagle Oil Co.*, 609 A.2d 11, 17 (N.J. 1992) (quoting RESTATEMENT 2D OF TORTS § 652B).

As a preliminary matter, Appellants' assertion that the elements of intrusion upon seclusion must be decided by a jury, Appellants' Brief at 51, ignores that the failure to plead elements sufficient to state a claim as a matter of law is grounds for dismissal of any claim; an intrusion upon seclusion claim is no different. *See, e.g.*, *Piscopo v. Pub. Serv. Elec. & Gas Co.*, No. 13-552, 2013 WL 5467112, at *9 (D.N.J. Sept. 27, 2013) ("Plaintiff argues that Defendants 'conduct[ed] surveillance on Plaintiff without consent or knowledge.' . . . Plaintiff's conclusory statement of surveillance is nothing more than a formulaic recitation of the elements of this tort. . . . Therefore, Plaintiff's tort claim of unreasonable intrusion upon seclusion is dismissed without prejudice."); *Swift v. United Food Commercial Workers Union Local 56*, No. L-2428-06, 2008 WL 2696174, at *3 (N.J. Super. Ct. App. Div. July 11, 2008) (affirming dismissal of intrusion upon seclusion claim for alleged privacy violations due to failure to allege even "basic and essential facts").

A claim for intrusion upon seclusion requires pleading that the defendant intentionally committed an intrusion he knew to be unlawful, as in the actor believing, or being "substantially certain, that he lacks the necessary legal or personal permission to commit the intrusive act." *O'Donnell v. United States*, 891 F.2d 1079, 1083 (3d Cir. 1989); *see also Jevic v. Coca Cola Bottling Co. of N.Y., Inc.*, No. 89-4431, 1990 WL 109851, at *8 (D.N.J. June 6, 1990).

Here, however, Appellants fail to allege that Viacom knew or was substantially certain that it lacked legal permission to place cookies on Appellants' computers. To the contrary, the lawful nature of the use of cookies has been established as far back as the *DoubleClick* opinion in 2001. Nor do Appellants allege that Viacom knew or was substantially certain that it lacked permission from Appellants to place cookies. By contrast, Viacom was and remains confident that its use of cookies violates no law. *See O'Donnell*, 891 F.2d at 1083.

In addition, Appellants had no reasonable expectation of privacy in wholly anonymous data generated by the website they voluntarily accessed. Under New Jersey law, an intrusion upon seclusion cannot occur "when the actor intrudes into an area in which the victim has either a limited or no expectation of privacy." *White v. White*, 344 N.J. Super. 211, 222 (N.J. Super. Ct. 2001) (finding no intrusion upon seclusion where a wife read her husband's emails stored on a family computer). There is no expectation of privacy in anonymous records of Internet

activity, which necessarily involves multiple parties (from an Internet service provider to a website operator).

Appellants' intrusion upon seclusion claim also fails because Viacom's actions were not highly offensive to a reasonable person as a matter of law. They did not violate any civil or criminal law. Appellants' allegations to the contrary are conclusory, *see* Appellants' Brief at 59, and entitled to no weight. Courts have consistently held that actions such as Viacom's are lawful and there is no basis to believe that Viacom's actions were highly offensive. *See also Tamayo v. Am. Coradious Int'l, LLC*, No. 11-cv-6549, 2011 U.S. Dist. LEXIS 149124, at *11–12 (D.N.J. Dec. 28, 2011) (finding that "bald assertions" that a defendant violated federal law do not suffice to establish highly offensive conduct).

To be clear, Viacom did not violate any of the statutes Appellants cite. *See* Appellants' Brief at 59–60. Viacom violated neither VPPA nor ECPA. *See supra* Sections I and II. Viacom did not violate the Pen Register Act because that Act relates solely to law enforcement activities and protects individuals being investigated for criminal conduct. *See* 18 U.S.C. § 3121 *et seq.* Viacom did not violate the Computer Fraud and Abuse Act because it did not cause damages in excess of $5,000 to Appellants' computers (indeed, it did not cause *any* damage). *See LaCourt*, 2011 WL 1661532.

Accordingly, Appellants' argument that Viacom's conduct was highly offensive relies on nothing more than generic public survey data. That is insufficient to support the allegation of offensiveness. Appellants must allege particular facts suggesting "conduct to which the reasonable man would strongly object." *Stengart v. Loving Care Agency, Inc.*, 201 N.J. 300, 317 (N.J. 2010). Claims involving only the anonymous collection of Internet data, solely to provide advertising, stand in stark contrast to the invasions of privacy that New Jersey courts have held to be "highly offensive":

- A claim that a coworker falsely reported that a teacher was threatening to kill people, leading to the teacher being taken to a hospital under police escort and subjected to psychiatric evaluations. *Leang v. Jersey City Bd. of Educ.*, 198 N.J. 557, 589–90 (N.J. 2009).
- A claim that a defendant installed hidden video cameras and recording equipment in bathrooms. *Soliman v. Kushner Cos.*, 433 N.J. Super. 153 (N.J. Super. Ct. 2013).
- A claim by a woman against her ex-boyfriend, who mailed sexually explicit pictures of the woman to her family in Christmas cards. *Del Mastro v. Grimado*, No. BER-C-388-03E, 2005 WL 2002355 (N.J. Super. Ct. Aug. 19, 2005).

These cases demonstrate that highly offensive conduct must exceed any reasonable expectation of privacy in a manner that would be strongly objectionable. *See Stengart*, 201 N.J. at 317. Viacom's use of cookies to anonymously record Appellants' communications with Viacom websites, by contrast, is nothing other than the lawful activity of countless commercial websites and, as a matter of law, cannot be highly offensive. *See In re DoubleClick*, 154 F. Supp. 2d at 502–03, 519 (noting that cookies are "commonly used by Web sites" and granting motion to dismiss).

CONCLUSION

This Court should affirm the well-reasoned decisions of the District Court below dismissing this case with prejudice.

Dated: June 15, 2015

/s/ Jeremy Feigelson

Jeremy Feigelson
David A. O'Neil
Christopher S. Ford
DEBEVOISE & PLIMPTON LLP
919 Third Avenue
New York, N.Y. 10022
(212) 909-6000
jfeigelson@debevoise.com
daoneil@debevoise.com
csford@debevoise.com

Stephen M. Orlofsky
BLANK ROME LLP
301 Carnegie Center, 3rd Floor
Princeton, N.J. 08540
(609) 750-7700
Orlofsky@BlankRome.com

CERTIFICATE OF COMPLIANCE
PURSUANT TO FED. R. APP. P. 32(a)(7)(C)

This brief contains 9,773 words, including headings, footnotes, and quotations, as calculated by Microsoft Word, and therefore complies with the requirements of Fed. R. App. P. 32(a)(7)(B).

/s/ Jeremy Feigelson

Jeremy Feigelson
DEBEVOISE & PLIMPTON LLP
919 Third Avenue
New York, N.Y. 10022
(212) 909-6000
jfeigelson@debevoise.com

CERTIFICATION OF BAR MEMBERSHIP

I hereby certify that I am a member of the bar of the United States Court of Appeals for the Third Circuit.

/s/ Jeremy Feigelson

Jeremy Feigelson
DEBEVOISE & PLIMPTON LLP
919 Third Avenue
New York, N.Y. 10022
(212) 909-6000
jfeigelson@debevoise.com

CERTIFICATION OF SERVICE

I hereby certify that, on June 15, 2015, I electronically filed the foregoing brief via the CM/ECF system for the United States Court of Appeals for the Third Circuit, which automatically sent a notification of such filing to all counsel of record.

As per Fed. R. App. P. 25(a)(2)(B)(ii), I sent copies of the foregoing brief to the Office of the Clerk of Court and to all Appellants' counsel of record for delivery within three days.

/s/ Jeremy Feigelson

Jeremy Feigelson
DEBEVOISE & PLIMPTON LLP
919 Third Avenue
New York, N.Y. 10022
(212) 909-6000
jfeigelson@debevoise.com

CERTIFICATION OF IDENTICAL BRIEFS

I hereby certify that the electronically filed version of this brief and the hard copies of the brief sent to the Clerk of Court and Appellants' counsel are identical.

/s/ Jeremy Feigelson

Jeremy Feigelson
DEBEVOISE & PLIMPTON LLP
919 Third Avenue
New York, N.Y. 10022
(212) 909-6000
jfeigelson@debevoise.com

CERTIFICATION OF VIRUS CHECK

I hereby certify that a virus check was performed on the electronically filed version of this brief using Symantec Anti-Virus Protection, and that no viruses were found.

/s/ Jeremy Feigelson

Jeremy Feigelson
DEBEVOISE & PLIMPTON LLP
919 Third Avenue
New York, N.Y. 10022
(212) 909-6000
jfeigelson@debevoise.com