UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 15-1441

In re: Nickelodeon Consumer Privacy Litigation

On Appeal from the U.S. District Court for the District Court of New Jersey
Case No. 2:12-cv-07829
The Honorable Stanley R. Chesler

APPELLANTS' REPLY BRIEF

EICHEN CRUTCHLOW
ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
Fax: (732) 248-8273

BARTIMUS FRICKLETON
ROBERTSON & GOZA
715 Swifts Highway
Jefferson City, MO 65109
Telephone: (573) 659-4454
Fax: (573) 659-4460

Co-Lead Counsel on Behalf of All Plaintiffs

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page**

Statutes

Other Authorities

LEGAL ARGUMENT

I. PLAINTIFFS SUFFICIENTLY PLEADED ART. III STANDING

a. PLAINTIFFS HAVE STATUTORY STANDING

Defendants argue standing requires proof – at the pleadings stage – of economic loss. The law provides otherwise. "A plaintiff need not demonstrate that he or she suffered actual monetary damages, because 'the actual or threatened injury required by Article III may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing.'" *Alston v. Countrywide Financial Corp.*, 585 F.3d 753, 763 (3d Cir. 2009).

Infringement upon a statutory right constitutes injury-in-fact for Article III standing purposes. The standard is whether that statute "grant[s] persons in the plaintiff's position a right to judicial relief." *Warth v. Seldin*, 422 U.S. 490, 500 (1975). That standard is met here.

The legislative history of the ECPA makes clear that Congress enacted these causes-of-action to remedy harm to constitutional rights:

> [T]he law must advance with the technology to ensure the continued vitality of the fourth amendment. Privacy cannot be left to depend solely on physical protection, or it will gradually erode as technology advances. Congress must act to protect the privacy of our citizens. If we do not, we will promote the gradual erosion of this precious right.

Senate Report ("S. Rep.") 99-541 (1986) at 5. In addition, the legislative history to the VPPA, S. Rep. 100-599 at 6, reveals the reasoning behind the private cause-of-action was to put "teeth into the legislation." *Id.* at 8.

If Plaintiffs come under the protection of these statutes, then they must have Article III standing to assert claims based upon them. *Id.* at 763; *Warth,* 422 U.S. at 500. Plaintiffs need not plead pecuniary loss for statutory standing. This resolves the standing inquiry in Plaintiffs' favor. *See Alston*, 585 F.3d at 759

Defendants' reliance on *Reilly v. Ceridian Corp.* and *Sterk v. Best Buy* is misplaced. In *Reilly*, the plaintiffs did not plead violations of statutes creating causes-of-action or intrusion upon seclusion to vindicate privacy rights. *Reilly v. Ceridien Corp.*, No. 10-5142, 2011 WL 735512 at *3 (D.N.J. 2011).

In *Sterk*, the plaintiffs failed to allege violation of the VPPA where the defendant disclosed personally identifiable information ("PII") to itself. The *Sterk* court held that the plaintiff did not submit "any competent proof that he ha[d] statutory standing under the VPPA" because he had only alleged that a subsidiary had "disclosed" PII to the parent corporation. The *Sterk* Court questioned whether violation of the statute alone was enough, but because the PII stayed within the company, the Court's language on non-statutory standing was dicta.

b. PLAINTIFFS HAVE COMMON LAW STANDING

Forty-seven states recognize the common law tort of Intrusion Upon Seclusion. Courts have long recognized that common law standing for privacy torts accrues upon the invasion of privacy itself and does not depend on allegations or proof of monetary harm. *Doe v. Chao*, 540 U.S. 614, 621 (2004). It is sufficient to allege intrusion alone because "[t]he tort is completed with the obtaining of the information by improperly intrusive means." *Pearson v. Dodd*, 410 F.2d 701, 704 (D.C. Cir. 1969). The fact that damages may not be capable of precise measure "by a pecuniary standard" is "not a bar to recovery." *Rhodes v. Graham*, 37 S.W.2d 46 (Ky. 1931). Viacom's argument that Plaintiffs need quantifiable damages at this stage misstates the law.

c. PLAINTIFFS ALLEGE SUFFICIENT ECONOMIC INJURY TO ESTABLISH INJURY-IN-FACT

Though not required, Plaintiffs alleged facts showing economic harm. The Supreme Court recognized that "[n]o social purpose is served by having the defendant get free some aspect of the plaintiff that would have market value and for which he would normally pay." *Zacchini v. Scripps-Howard Broadcasting Co.*, 433 U.S. 562 (1977). The Complaint alleges violation of Plaintiffs' financial interests to support their allegations that PII has monetary value, and is the primary commodity Defendants trade and sell. Plaintiffs' Second Consolidated Class Action Complaint ("*Second CAC*"), *App'x* 2 at 71-74. At the pleading stage, the District Court must

accept those allegations as true. *Ballentine v. U.S.,* 486 F.3d 806, 810 (3d Cir. 2007). These allegations are sufficient to show economic injury at the pleading stage.

II. PLAINTIFFS SUFFICIENTLY STATED A CLAIM UNDER THE VPPA

The VPPA defines PII to "include[] information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." The District Court of Massachusetts explained how and why the information disclosed by Viacom in this case is personally identifiable under the Act. *Yershov v. Gannett Satellite Info. Net.*, No. 14-13112, 2015 WL 2340752 (D. Mass. May 15, 2015). In *Yershov*, the plaintiffs alleged VPPA violation where the defendant, a smart-phone app producer, disclosed users' video-viewing histories and unique device identifiers to the third-party data company Adobe.

Here, Plaintiffs' *Second CAC,* alleged disclosure of far more information from Viacom to Google – including each child's: (1) unique username or alias; (2) gender; (3) age/birthdate; (4) IP address; (5) browser settings; (6) unique device identifier; (7) operating system; (8) screen resolution; (9) browser version; (10) the content of the child's web communications, including but not limited to the detailed URL requests and videos requested from Viacom's children's websites; and (11) a unique DoubleClick persistent cookie identifier used by Google to track communications. *Second CAC, App'x* 2 at 152-53.

Like Viacom here, the *Yershov* defendant argued it had not disclosed PII because the information disclosed could not be linked to a specific person without access to additional information. The *Yershov* Court rejected this argument, recognizing that claim "is true of every identifier other than a person's name." In commenting on the District Court's decision in this case, the *Yershov* Court explained:

> *Nickelodeon's* conclusion that 'PII is information which must, without more, itself link an actual person to actual video materials' is flawed. That conclusion would seemingly preclude a finding that a home address or social security number is PII. Surely, that cannot be correct.

Yershov 2015 WL 2340752, at *8.

Recognizing the implications that *Yershov*'s reasoning may have on this appeal, Viacom attempts to distinguish it. However, Viacom's argument that "Appellants allege disclosure of a cookie-based UUID" is counter-factual to the Plaintiffs' petition, which alleged disclosure of 11 separate items, including a unique device identifier. *Second CAC, App'x* 2 at 152-53.

The VPPA does not state anywhere that PII disclosures must also be information collected directly by a video-tape service provider ("VTSP"). Yet, in its brief, Viacom misstates the text of the VPPA by claiming it only applies to disclosures by VTSPs of "information that they have collected." *Viacom Brief* at

14-15.[1] Those words are not in the VPPA. The purpose of the VPPA is to protect consumer video-viewing histories, and Congress drafted the legislation to ensure it could keep pace with technology.

Defendant Viacom also argues that the VPPA does not prohibit the disclosure of information that only "theoretically could be used by the recipient to identify the location of a connected computer." *Viacom Brief* at 16. However, the *Second CAC* is based on public admissions from Defendant Google on its ubiquity, not theory or conjecture. For example, Google:

- Admits it connects persistent cookie identifiers, IP addresses, and unique device identifiers with user information in server logs. *See Second CAC, App'x* 2 at 136-137;
- Informs users, "We anonymize this log data by removing part of the IP address (after 9 months) and cookie information (after 18 months)." *Id.* at 137
- Admitted through its Privacy Director that IP addresses are personally-identifiable to companies with information like that which Google retains in its "server logs." *Id.*
- Defines "personal information" in its own Privacy Policy to include IP addresses and cookie identifiers, "information which you provide to (Google)

[1] Defendant Viacom mistakenly claims "Appellants concede, as they must, that Viacom did not knowingly disclose to Google any information that identifies a specific person." *Viacom Brief* at 16. Appellants made no such concession.

which personally identifies you, such as your name, email address, or billing information, or other data which can be reasonably linked to such information by Google." *Plaintiffs' Brief* at 21.

Viacom piggybacks its misstatement of the text of the VPPA by claiming it "cannot 'knowingly' disclose that which it does not know." *Viacom Brief* at 19. But Viacom knows of Google's ubiquity and Plaintiffs' *Second CAC* pleads as much. *Second CAC, App'x* 2 at 130-131.

In previous litigation between these same Defendants, both publicly acknowledged that usernames and persistent identifiers (including IP addresses) constitute PII. *Viacom v. YouTube*, Case Nos. 07-cv-2103 and 07-cv-3582 (S.D. N.Y.). In *Viacom v. YouTube*, an issue arose over whether Google should be required to disclose to Viacom the usernames and IP addresses of YouTube users connected to those same users' video viewing histories. Following public outcry, the Defendants agreed that usernames and IP addresses were PII that necessitated shielding from discovery. Viacom explained that, under the stipulation, "[t]he personally identifiable information that YouTube collects from its users [would] be stripped from the data before it [was] transferred to Viacom."[2] The stipulation filed

[2] Viacom Statement on Confidentiality of YouTube Data – 7/7/2008, which had been available at http://news.viacom.com/news/Pages/youtubeconfidentiality.aspx as of Feb. 16, 2014. It was deleted from Viacom's webpage after Plaintiffs cited it in briefing before the District Court, but remains available at:

with the District Court then provided that YouTube would strip PII by using "substitute values" for User IDs, IP Addresses, and Visitor IDs – a list which is narrower than that which Plaintiffs allege was disclosed here. Viacom and Google rightfully took steps to protect the PII of YouTube video viewers during their own dispute, and this Court should hold them to the same standard here. *See Viacom Int'l, Inc. v. YouTube and Google* (U.S.D.C. S.D. N.Y., Case No. 1:07-cv-02103) (Filed 3/13/07) Docket No. 119.

Additionally, Viacom's argument that Google's promise not to "combine DoubleClick cookie information with PII" immunizes parties from liability under the VPPA has no statutory support. There simply is no "third party promise" exception in the law.

Viacom further claims that identification of the minor children Plaintiffs through information Google has collected about their parents is not enough to "identif[y] a person" under the VPPA. *Viacom Brief* at 21. This ignores the breach of privacy that led Congress to enact the VPPA. "The impetus for [the VPPA] occurred when a weekly newspaper in Washington published a profile of Robert H. Bork based on the titles of 146 files *his family had rented* from a video store." S. Rep. 100-599 at 6 (1988).

---

https://web.archive.org/web/20120606043643/http://news.viacom.com/news/Pages/youtubeconfidentiality.aspx

Viacom's reliance on *Pichler v. UNITE*, 542 F.3d 380 (3d Cir. 2008) is also misplaced. There, the Third Circuit held that the Driver's Privacy Protection Act ("DPPA") only protected the privacy interests of "the individual" whose personal information from their motor vehicle records is at issue. In *Pichler*, five plaintiffs successfully prosecuted actions under the DPPA against a defendant who obtained the plaintiffs' driver's license numbers, used that information to request the plaintiffs' driving records, then used those records to attempt to recruit them. Among the successful plaintiffs were Russell Daubert and Jose Sabastro. The District Court dismissed claims of Carri Daubert and Deborah Sabastro, who alleged that the defendant's misuse of their husbands' driving records also revealed their shared addresses. Because "neither Carri Daubert nor Deborah Sabastro were the registered owners of the vehicles about which [the defendant] obtained information, they suffered no invasion of an interest" protected by the DPPA. *Pichler,* 542 F.3d at 391.

Viacom argues *Pichler* "stands for the proposition that a connect-the-dots approach . . . is beyond the scope of the statute." *Viacom brief* at 22-23. But Viacom ignores that *Pichler* found liability where the defendant connected-the-dots between plaintiffs' license numbers and other information.

In reality, *Pichler* holds that a plaintiff whose driving record is not misused under the DPPA is precluded from suit. That is not the situation here, as Plaintiffs had their video-viewing histories disclosed.

Finally, this Court must see through the slippery-slope argument from Viacom and amicus which characterize Plaintiffs' claims as a broad-side attack on Internet cookies. *See Viacom Brief* at 22-23. Plaintiffs do not challenge the validity of Internet cookies in general, only the way they are misused by Defendants here.

The legality of persistent tracking cookies depends upon explicit or implied user consent. The first major cookies case involved DoubleClick, now a Google subsidiary, which served the very cookies at issue here. In *In re: DoubleClick Privacy Litig.*, 154 F.Supp.2d 497, 505 (S.D. N.Y. 2001), the Court upheld tracking cookies on the theory of implied consent. Nearly all tracking cookies comply with the result reached in the DoubleClick case. Those cookies are ordinary and non-controversial.

The present case is different in three ways. First, it involves knowingly tracking the communications of millions of minor children who, as a matter of law, *are incapable of consent*, and whose communications are simultaneously protected by the Children's Online Privacy Protection Act. Second, this case involves disclosures to Google that personally-identify the minor children because of

Google's ubiquity. Third, it involves the VPPA, which has a particular method for obtaining "informed, written consent."

Additionally, Plaintiffs do not seek to change or hinder honest, ethical and legal Internet commerce in any way. In fact, as alleged in Plaintiffs' *Second CAC*, Defendant Viacom has revamped its Nick.com website so that it *no longer discloses the particular video viewing or game histories of individual users of Nick.com to Google*. Despite these changes to comply with the law, Viacom and the Nickelodeon websites continue to function.

Moreover, the amicus contorts the legislative history of the VPPA by arguing that the Act "does not extend to the sharing of cookies, IP addresses, and 'anonymous' demographic data like gender and age" or online data privacy. In 2012, the VPPA was updated to allow Internet VTSPs an easier method of obtaining "informed, written consent." S. Rep. 112-258 (2012) at 1. The amendments to the VPPA became law in January 2013, more than six months after the Court in *In re: Hulu Privacy Litigation* permitted the plaintiffs to proceed on VPPA claims against a VTSP who provided streaming services over the Internet. *In re: Hulu*, No. C 11-03764 LB (N.D. Cal. June 11, 2012). It is the amicus and the Defendants, not the Plaintiffs, who seek to change the nature of the VPPA. Having failed in 2012 to amend the VPPA to exclude streaming services over the Internet, Defendants and

the amicus now ask this Court to do what they do not have the political power to do in Congress. This Court should reject their effort.

III. PLAINTIFFS SUFFICIENTLY STATED A CLAIM UNDER THE FEDERAL WIRETAP ACT

The Wiretap Act prohibits intentional interception of contents of an electronic communication using a device either (1) without the lawful consent of a party to the communication; or (2) with a tortious or criminal intent. There are three issues before the Court on this claim:

- First, whether URLs containing video names and titles include "content," or, in the actual language of the Act – whether they contain "any information concerning the substance, purport, or meaning" of a communication;
- Second, whether Viacom can legally consent to a third party's interception of its communications with minor children; and
- Third, whether Defendants' interceptions were done with tortious or criminal intent.

a. URLS CONTAIN "CONTENT"

"Contents" are broadly defined to include "any information concerning the substance, purport, or meaning" or an "electronic communication." 18 U.S.C. § 2510(8). Here, Plaintiffs alleged interception of detailed URLs containing the names of requested and viewed videos and games on Viacom's websites, as well as detailed URLs on other websites, and the Plaintiffs' personal information. *See* Master

Consolidated Class Action Complaint ("*First CAC*"), *App'x* 2 at 90-95, 97-98; *Second CAC, App'x* 2 at 130-31, 140-41. Plaintiffs' Complaints included the following examples:

- http://www.nick.com/shows/penguins-of-madagascar
- http://www.wikihow.com/Deal-With-Your-Parents'-Divorce
- http://www.nick.com/videos/clip/digital-short-penguins-of-madagascar-shorts-skippers-nightmare.html

Viacom's claim that a URL "is not the substance, purport, or meaning of a communication" misstates the law. *Viacom Brief* at 35. By its plain terms, "content" need not include the entire communication itself, but instead must only contain "*any* information *relating* to the substance, purport, or meaning." *Declassified FISC Opinion, App'x* 2 at 323. The URLs above, and others with the titles of video clips, unquestionably fit this definition.

Viacom's brief also confuses the holding in *Zynga*, where the Ninth Circuit explained that URLs contain content in circumstances where they include "a search term or similar communication" made by a user. *In re: Zynga Privacy Litig.*, 750 F.3d 1098, 1109 (9th Cir. 2014). The URLs at issue in *Zynga* were Facebook URLs that only included the name of a person or group. The URLs here are different. They include the names of video requests in Plaintiffs' GET requests to Viacom. These are "similar communications" in that they are purposeful requests for specific media

that involve a conscious choice by the user to request information from Viacom or other websites.

Viacom's related argument that, 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 might theoretically protect," is likewise contrary to the plain language of the statute. *Viacom Brief* at 36. In a similar situation, courts have held that email subject lines contain "content" under the Wiretap Act, even though they do not include the text of a communication. *See In re: Application for an Order Authorizing a Pen Register and a Trap & Trace Device on Email Account*, 416 F.Supp.2d 13, 19 (D.C. Dist Ct. 2006) and *Optiver Australia Pty. Ltd. v. Tibra Trading Pty.*, No. 12-80242, 2013 WL 256771, at *2 (N.D. Cal. Jan. 23, 2013). Likewise, this Court should conclude that the URL's Plaintiffs alleged Defendants intercepted are "contents" under the Wiretap Act.

b. VIACOM CANNOT LAWFULLY CONSENT TO THIRD PARTY INTERCEPTIONS OF COMMUNICATIONS WITH MINORS

Defendants contend that the age of a party whose communications are intercepted is irrelevant because the Federal Wiretap Act is a single-party consent statute. However, a minor's ability to contract and consent to an agreement has

never been treated in the same way as an adult. The age of a minor is "more than a chronological fact." *Eddings v. Oklahoma*, 455 U.S. 104, 115 (1982).

Both Viacom and Google understood they were tracking communications of minor children legally incapable of consent. After all, the very purpose of the website at issue, Nick.com, is to market to children viewing the Nickelodeon television network. Plaintiffs propose that the applicable rule here should be that "when one party to a conversation is under the age of eighteen, the only person who can consent to an interception is a . . . judge" or parental guardian. *Bishop v. State*, 241 Ga. App. 517, 522 (1999).

c. VIACOM AND GOOGLE'S INTERCEPTIONS WERE ACCOMPLISHED WITH TORTIOUS AND CRIMINAL INTENT

Even though Viacom was a party to the intercepted communications, it is outside the statutory exception because their purpose in intercepting the communication was done with tortious or criminal intent. *See infra Section VIII; Caro v. Weintraub*, 618 F.3d 94 (2d Cir. 2010).

d. GOOGLE WAS NOT AN AUTHORIZED PARTY TO THE COMMUNICATION

The Wiretap Act provides an affirmative defense to any person who is an authorized party to a communication. 18 U.S.C. § 2510(d)(2). Defendants' bear the burden of establishing this affirmative defense. *In re: Pharmatrak*, 329 F.3d 9, 19 (1st Cir. 2003).

Google asserts that the minor Plaintiffs understood when they clicked on a link to watch a video at Nick.com that they were somehow authorizing Google to receive the same communication. *Google Brief* at 29. Consent or authorization "should not be casually inferred" in ECPA claims, particularly at the motion to dismiss stage when the Court must take all well-pleaded fact as true." *In re: Pharmatrak*, 329 F.3d at 20. Just as a medical patient may consent to one form of treatment but refuse another, so too may a party consent to access to "only a subset of its communications." *Id.* at 19. Defendants cannot manufacture their own exemption to the Wiretap Act by taking advantage of minor children. *In re: iPhone Application Litig.*, 844 F.Supp. 2d 1040, 1062 (N.D. Cal. 2012).

Moreover, Defendants' attempt to silo the cookie value from the other information it would allegedly receive anyway must be rejected. Even if some communications were voluntary, the use of the tracking cookie enabled the gathering of far greater content than otherwise contemplated and understood by the minor Plaintiffs. It is a difference in kind, as opposed to degree. The minor childrens' browsers "sent different information in response to targeted advertising than would have been sent without the setting of third-party cookies. For this reason also, Google is not appropriately deemed a party to the communications." *In re: Google Cookie Placement Consumer Privacy Litig.*, 988 F.Supp.2d 434, 443 (D. Del. 2013).

e. DEFENDANT VIACOM IS LIABLE FOR PROCUREMENT

Viacom argues procurement liability is impermissible under the Wiretap Act. This is incorrect. *See Lonegan v. Hasty*, 436 F.Supp.2d 419, 428 (E.D. N.Y. 2006) (holding procurement liability still exists under ECPA). The *Lonegan* court emphasized that "the more natural reading of the amended statute shows no intent on the part of Congress to eliminate the private right of action for procurement violations." *Id.* The *Lonegan* court conducted a thorough analysis of the legislative history and concluded that "Congress intended to streamline the language of the provision . . . but that it did not, in so doing, intend to eliminate procurement violations from civil liability." *Id.* Plaintiffs may thus pursue a claim against Viacom for procuring Google to violate Plaintiffs' rights under the ECPA.

IV. PLAINTIFFS SUFFICIENTLY PLEADED VIOLATION OF CIPA

The elements of a California Invasion of Privacy Act claim are identical to a Federal Wiretap claim, with one exception. To prevail under CIPA, a defendant must show consent from *all* parties to a communication, including the plaintiff. Cal. Penal Code § 631(a). Plaintiffs here are minors, incapable of consent. They alleged lack of consent by themselves as well their parents or guardians. *Second CAC, App'x* 2 at 128. Thus, they have adequately stated a CIPA claim.

V. PLAINTIFFS SUFFICIENTLY STATED A CLAIM UNDER THE SCA

The Stored Communication Act ("SCA") prohibits intentional access exceeding authorization to a "*facility* through which an electronic communication service ("ECS") is provided" and that results in access to a communication in electronic storage. 18 U.S.C. § 2701(a). By the SCA's plain language, determining a "facility" is a two-part inquiry. First, a court must ask what the relevant ECS is. Second, it must determine those things, i.e. facilities, "through which" the ECS is provided.

a. ISPs AND WEB-BROWSERS ARE ELECTRONIC COMMUNICATION SERVICES

The SCA defines an ECS as "any service which provides to users thereof the ability to send or receive wire or electronic communications." Plaintiffs alleged two relevant ECSs: their Internet Service Providers (which Google does not challenge as an ECS) and their web-browsers. *First CAC, App'x* 2 at 99-100.

Google argues that a web-browser is not an ECS because a browser cannot grant or revoke authorization to use the service, have officers or employees, or be subject to court orders or judgments. *Google Brief* at 38-39. First, Google misstates the actual text of the SCA. Nothing in the statutory definition requires an ECS to do those things. Second, Google attempts to inject disputed facts, which are contradicted by its own pronouncements concerning its web-browser.

i. Web-Browsers Provide a Service

Google describes the web-browser as "the most important software on our computer."[3] On the launch of its own web-browser Google explained:

> All of us at Google spend much of our time working inside a browser. We search, chat, email and collaborate in a browser. And in our spare time, we shop, bank, read news and keep in touch with friends -- all using a browser.[4]

Searching, chatting, emailing, collaborating, shopping, and keeping in touch with friends over the Internet all involve electronic communications – and, as Google explains above, all of those communications are accomplished "using a browser." In addition, every web-browser of which Plaintiffs are aware includes a "Terms of *Service*," including Google Chrome.[5]

ii. Web-Browser Companies Are Capable of Doing All the Things Google Claims They Can Not

Web-browsers are not stand alone entities. They are services owned and operated by companies. As alleged in Plaintiffs' *First and Second CAC*, popular web-browsers include *Apple* Safari, *Microsoft* Internet Explorer, *Google* Chrome, and *Mozilla* Firefox. These companies have agents and employees, are subject to court orders, and can grant or revoke authorization to use their services. Google's Terms of Service for Chrome informs users that it may grant third-party developers

[3]http://chrome.blogspot.com/2009/04/11-short-films-about-browser.html
[4]http://googleblog.blogspot.com/2008/09/fresh-take-on-browser.html

"greater privileges to access your browser or your computer than regular webpages, including the ability to read and modify your private data" and that these third-party "extensions" may be updated through "downloading and installing" updates "without further notice" to the user.[6]

b. PLAINTIFFS' COMPUTING DEVICES AND BROWSER-MANAGED FILES ARE THE FACILITIES THROUGH WHICH THE ELECTRONIC COMMUNICATION SERVICES OF ISPs AND WEB-BROWSERS ARE PROVIDED

Though courts are split on the "facilities" issue, the decisions Google urges this Court to follow mistakenly conflate the definition of ECS with "facility." Under the plain terms of the statute, a "facility" is neither the same thing as an ECS, nor does it have to be an item owned by an ECS. Instead, a "facility" is that "through which an ECS is provided."

This broad definition of "facility" makes sense when considering the purpose of the SCA, which was enacted "because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address." *Crispin v. Christian Audiger, Inc.*, 717 F.Supp.2d 965, 971 (C.D. Cal. 2010). It was meant to amend previous law considered "hopelessly out of date" and that had "not kept pace with the development communications and computer technology." S. Rep. 99-

---

[6] *See* Google Chrome Terms of Service at ¶20, *available at*: https://www.google.com/chrome/browser/privacy/eula_text.html.

541 (1986) at 2. In employing these definitions, Congress enabled the ECPA to adapt to changes in technology.

VI. COPPA DOES NOT PRECLUDE PLAINTIFFS' STATE LAW CLAIMS

Viacom argues that Plaintiffs' state law claims are expressly preempted by the Children's Online Privacy Protection Act ("COPPA"). Federal law preempts state law where: (1) the federal statute expressly states so ("express preemption"); (2) Congress preempts the entire field of law ("field preemption"); or (3) the state and federal laws require conflicting or inconsistent compliance ("conflict preemption"). *See Arizona v. U.S.*, 132 S.Ct. 2492, 2500-01 (2012). Here, Viacom claims express preemption.

COPPA requires an "operator of any website or online service" to obtain parental consent before it collects or uses the "personal information" of a "child," where the child is "under the age of 13." *See, e.g.*, 15 U.S.C. §§6501(1), 6502(a), 6502(b)(1)(A)(iii), 16 C.F.R. part 312. COPPA provides that "[n]o State or local government may impose any liability for . . . activities or actions by operators . . . in connection with an activity or action described in this chapter that is *inconsistent with* the treatment of those activities or actions under this section." *Id.* at §6502(d).

In conclusory fashion, Viacom argues Plaintiffs' state-law claims are "expressly preempted by federal law." *Viacom Brief* at 38. Thus, Viacom impermissibly extrapolates that the statute – which Congress believed necessary to

provide a safer, more secure online experience for children – expressly preempts all state-law claims brought by those same children.

While COPPA includes an express preemption provision, at least with respect to "inconsistent" state law, the existence of such a provision alone does not end the inquiry. *See, Farina v. Nokia, Inc.*, 625 F.3d 97, 118 (3d Cir. 2010), *cert. denied* 132 S.Ct. 365 (2011) (confirming presence of express preemption provision does not end inquiry); *Medtronic, Inc. v. Lohr*, 518 U.S. 470, 484-85 (1996) (same). While courts need not inquire whether Congress intended to preempt some state law, courts still must examine congressional intent as to the scope of the preemption provision. See, *Lohr,* 518 U.S. at 485-86. Thus, the task is to identify the domain expressly preempted, because "an express definition of the pre-emptive reach of a statute . . . supports a reasonable inference . . . that Congress did not intend to preempt other matters." *See Freightliner Corp. v. Myrick*, 514 U.S. 280, 288 (1995); *Cipollone v. Liggett Group, Inc.*, 505 U.S. 504, 517 (1992).

The Court's analysis must be guided by two cornerstones of preemption jurisprudence. *Wyeth v. Levine*, 555 U.S. 555, 565 (2009); *see also*, *Farina*, 625 F.3d at 115. First, "the purpose of Congress is the ultimate touchstone in every preemption case." *Lohr*, 518 U.S. at 485. Second, "[i]n all preemption cases, and particularly in those in which Congress has 'legislated . . . in a field which the States have traditionally occupied,' . . . [courts] 'start with the assumption that the historic

police powers of the States were not to be superseded by the Federal Act unless that was the clear and manifest purpose of Congress." *Id.* (*quoting Rice v. Sante Fe Elevator Corp.*, 331 U.S. 218, 230 (1947)). That is, there is a "presumption against preemption," which specifically applies in a field within the police power of the state. *Wyeth*, 555 U.S. at 555, n.3; s*ee also Lohr*, 518 U.S. at 475, 485. Thus, this Court's analysis starts with a presumption that Congress did not preempt all state-law claims by enacting COPPA.

The issue is whether Viacom has overcome that presumption by demonstrating a clear Congressional purpose to preempt or that the existence of a conflict between state and federal law is "clear and manifest." *See Farina*, 625 F.3d at 117 (*citing Fellner v. Tri-Union Seafoods LLC*, 539 F.3d 237, 249 (3d Cir. 2008), *cert. denied*, 129 S.Ct. 1987 (2009)). Viacom has shown neither.

Moreover, an examination of the purpose of COPPA makes manifest that the Act does not preempt all state laws. COPPA was enacted to enhance parental involvement in a child's online communications, protect children's online safety, secure children's PII, and limit information collection absent parental consent.[7]

To effectuate these goals, Congress included five key requirements: (1) notice; (2) parental consent; (3) parental review; (4) limitations on the use of games

[7] Notice of Proposed Rulemaking and Request for Public Comment, 64 FR 22750 (Apr. 27, 1999), citing 144 Cong. Rec. S12741 (daily ed. Oct. 7, 1998) (Sen. Bryan Statement).

and prizes; and (5) security. 15 U.S.C. §§6502(b)(1)(A-D); *see also* 16 CFR §§312.4(b)-312.8. And, while Congress included a limited preemption provision, the purpose of that provision was not to preclude all state regulation of children's online privacy, but to prevent state and local governments from adopting requirements inconsistent with those imposed by COPPA. 15 U.S.C. §6502(d).

Here, Plaintiffs' state law claims do not seek to impose liability for activities that are inconsistent with those set forth in COPPA. To the contrary, Plaintiffs' state law privacy claims are based on Viacom's collection and use of personal information without parental consent. Those claims are entirely consistent with COPPA's mandate that operators of websites/online services obtain parental consent for the collection, use or disclosure of personal information from children. 15 U.S.C. §6502(b)(1)(A)(ii). Further, Plaintiffs' *Second CAC* cites COPPA standards (and Defendants' violations of them). *Second CAC, App'x* 2 at 150, 160-61. Plaintiffs' state law claims are not "inconsistent with" the activities covered by COPPA.

Simply put, COPPA was not intended to preempt state law claims based on duties that are consistent with the Act. As drafted, §6502(d) signifies that Congress did not intend to preempt all state law, and Viacom's preemption claims should be rejected.

VII. PLAINTIFFS STATED A DAMAGE APPLICABLE TO THE NEW JERSEY COMPUTER RELATED OFFENSES ACT

Defendants allege that Plaintiffs have not shown damage in business or property, because Plaintiffs do not specify a monetary figure.[8] *Viacom Brief* at 39-40. This is incorrect. Nothing in the NJCROA requires Plaintiffs affix a precise value to their damages at the pleading stage. Rather, Plaintiffs need only state a reasonable basis for damage, which Plaintiffs have done through allegations of unjust enrichment. *See Goldsmith*, 975 A.2d 459, 463 (N.J. App. Div. 2009).

Viacom notes that unjust enrichment has never been used as a measure of damages under the NJCROA, but that is a far cry from concluding – without legal authority – that such a remedy is precluded. On the other hand, there is lengthy support for the notion that unjust enrichment is an acceptable measure of damages from a quasi-contractual standpoint. *See, e.g. Goldsmith*, 975 A.2d at 46.

In a quasi-contract "there is no agreement; but they are clothed with the semblance of contract for the purpose of the remedy, and the obligation arises not from consent, as in the case of true contracts, but from the law or natural equity."

[8] Google recycles its Motion to Dismiss arguments already addressed in Plaintiffs' Opposition. *See* U.S.D.C D.N.J., Case No. 2:12-cv-07829 (Filed Dec. 24, 2012) Docket Nos. 78, 81. Plaintiffs rely on their previous submissions as these issues are not on appeal, nor raised in Plaintiffs' Opening Brief. The issue raised by the District Court deals solely with Plaintiffs damage "in business or property". *See* January 20, 2015 Decision of the District Court, App'x 1 at 53-54; *see also* Concise Summary of the Case, Document 003111898186 filed on March 9, 2015.

Callano v. Oakwood Park Homes Corp., 219 A.2d 332, 334 (N.J. App. Div. 1966). Usually, a contract defines the duty, but "in the case of quasi-contracts the duty defines the contract . . . . The duty which thus forms the foundation of a quasi-contractual obligation is frequently based on the doctrine of unjust enrichment." *Id.*

Here, Defendants repeatedly allege that Plaintiffs consented to the use of Defendants' cookies. Even though Plaintiffs challenge the validity of a minor's ability to consent, it does not change the fact that Defendants themselves use the contractual term "consent" to describe the situation. Defendants should not be permitted to claim a contractual agreement on one hand and on the other suggest no contract exists with which to measure damages. Plaintiffs have demonstrated an injury in business or property as required by the NJCROA.

VIII. INTRUSION UPON SECLUSION

The common law tort of intrusion upon seclusion requires: (1) an intentional intrusion; (2) upon the solitude or seclusion of a plaintiff and their private affairs; which would be (3) highly offensive to a reasonable person. *Restatement (Second) of Torts* § 652B. All elements are met here.

a. DEFENDANTS' CONDUCT WAS *INTENTIONAL*

Defendant Viacom claims it cannot be held liable because it neither "knew or was substantially certain that it lacked legal permission to place cookies on Appellants' computers." In this context, ignorance is no excuse.

First, §652B of the Restatement (Second) does not "require a complainant to have knowledge of the reasons for the intrusion. Rather, the intentional intrusion itself . . . is sufficient to establish these torts." *Yates v. CIB, Inc.*, 81 F.Supp. 2d 546, 551 (E.D. Pa. 2012). Second, the knowing commission of an illegal act is, by definition, highly offensive to a reasonable person. Defendants' effort to invoke a scienter requirement would render the tort's "highly offensive" element meaningless. Third, the issue of Defendants' knowledge of the legality of its own conduct would require extensive fact-finding, making dismissal premature.

Further, the cases relied upon by Defendants, *O'Donnell v. U.S.*, 891 F.2d 1079 (3d Cir. 1989) and *Jevic v. Coca-Cola Bottling Co.*, No. 89-4431, 1990 WL 109851 (D.N.J. 1990) do not establish that intrusions are permissible unless known by the intruder to be unlawful. Instead, these cases explain that "to intrude, in the tort context, one must act without permission." *Jevic*, 1990 WL 109851 at *8. In both *O'Donnell* and *Jevic*, there was no dispute that the defendants had permission to commit the intrusive acts. *See O'Donnell*, 891 F.2d at 1081, 1083; *Jevic*, 1990 WL 109851 at *9-10; s*ee also Gibbs v. Massey*, No. 07-3604, 2009 WL 838138 at *11 (D.N.J. March 26, 2009) ("The linchpin of the intrusion element is that it must be committed without consent.").

Here, Defendants neither received nor sought consent to deliberately gather PII from millions of children. Even if these children could voluntarily provide their

usernames and registration information, no one authorized Defendants to intercept, track, record, and disseminate their communications.

b. DEFENDANTS' INTRUSIONS WERE NOT ANONYMOUS

Viacom argues Appellants "had no reasonable expectation of privacy in wholly anonymous data generated by the website they voluntarily accessed." *Viacom Brief* at 42. This misstates the nature of the information Viacom collected and then disclosed to Google – and the information Google used to track the Plaintiffs. The information at issue here was not anonymous. As explained by *Yershov*, *supra*, referring to the identifiers in this case as "anonymous" is "unhelpful and possibly misleading." For example, *Yershov* pointed out, "a social security number or a date of birth, in isolation, is anonymous. However, it would be absurd to conclude that a social security number is not PII[.]"

c. A REASONABLE PERSON COULD FIND DEFENDANTS' INTRUSIONS HIGHLY OFFENSIVE

"[R]easonableness (and offensiveness) are highly fact-sensitive inquiries" which "are not properly resolved on a motion to dismiss." *Ehling v. Monmouth-Ocean Hosp. Service Corp.*, 872 F.Supp.2d 369, 374 (D.N.J. 2012). To prevail on their argument that intrusions were not highly offensive as a matter of law, Defendants must show that no reasonable person could find their behavior highly offensive. Plaintiffs' inclusion of public surveys on Internet tracking and the tracking of children reveal that a reasonable person could find Defendants' conduct

highly offensive. Additionally, Plaintiffs' *Second CAC* includes facts to show violations of not only the VPPA, Wiretap Act, and SCA as explained above, but also violations of the Pen Register Act, the Computer Fraud and Abuse Act and its state-based equivalents in all 50 states. A reasonable person, made aware that Defendants violated federal and state-based criminal laws could find these intrusions highly offensive.

Viacom's claim that "[c]ourts have consistently held that actions such as Viacom's are lawful" ignores the critical fact that there are no cases governing the use of cookies to knowingly track minor children without their parents' consent. The same is true for Google's citation to a series of cases involving cookies on websites geared towards adults. *Google Brief* at 60. Indeed, every cookie case on which Defendants rely involve adults who consented to tracking. Children cannot lawfully consent on their own – and neither Viacom nor Google took any steps to gain parental consent. To Plaintiffs' knowledge, there are no Internet cookies cases, nor any cases involving acts that violate federal and state criminal laws, where the victims are millions of American children.

Viacom's claim that the Pen Register Act "relates solely to law enforcement activities and protects individuals from being investigated for criminal misconduct" misstates the law. *Viacom Brief* at 43. The Act applies to all persons, not just law enforcement. *See* 18 U.S.C. § 3121(a). Violation of the Act is subject to a criminal

penalty of a fine or one year in prison. 18 U.S.C. §3121(d). Plaintiffs plead sufficient facts to show violation of the Pen Register Act. A "pen register" is defined under the Act as "a device or process which records or decodes dialing, routing, addressing, or signaling information . . . provided, however, that such information shall not include the contents of any communication." 18 U.S.C. §3127(3). As explained in Plaintiffs' Wiretap section, a URL may contain both dialing, routing, addressing and signaling ("DRAS") information and content. The Defendants argue it is DRAS only. Plaintiffs explain how it is both. But there is no dispute that it includes DRAS. As such, it is protected by the Pen Register Act – and Defendants have violated both it and the Wiretap Act.

Viacom argues it did not violate the Computer Fraud and Abuse Act ("CFAA") because it did not cause damages in excess of $5,000 to Appellants' computers. *Viacom Brief* at 43. This confuses the automatic statutory cause-of-action under the CFAA with the criminal portion of the Act. The elements of a criminal CFAA violation, as alleged here, are: (1) intentional; (2) access; (3) to a computer; (4) without authorization or exceeding authorization; and thereby (5) obtaining information from; (6) a computer used in interstate commerce or communication. 18 U.S.C. §1030(a)(2)(C). Under the punishment section, violators are subject to a fine or imprisonment for up to a year for a first offense. 18 U.S.C. §1030(c)(2)(A). There is no $5,000 threshold.

Finally, Google's argument that it did not understand that it was tracking minor children on the Viacom websites is highly questionable. *Google Brief* at 66. Nickelodeon is a television station focused solely on children and Nick.com is a children's website devoted to programming on Nickelodeon. Google was aware of that just as much as Viacom, and both should be liable for violating the statutes above for preying on unsophisticated minors.

CONCLUSION

For the aforementioned reasons, Plaintiffs respectfully request that this Court reverse the District Court.

Respectfully Submitted,

/s/ Barry R. Eichen
Barry R. Eichen
Evan J. Rosenberg
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
beichen@njadvocates.com
erosenberg@njadvocates.com

James P. Frickleton
Edward D. Robertson III
BARTIMUS FRICKLETON ROBERTSON & GOZA, PC
11150 Overbrook Rd., Suite 200
Leawood, KS 66211
Telephone: (913) 266-2300
jimf@bflawfirm.com
krobertson@bflawfirm.com

Edward D. Robertson, Jr.
Mary D. Winter
BARTIMUS FRICKLETON ROBERTSON & GOZA, PC
715 Swifts Highway
Jefferson City, MO 65109
Telephone: (573) 659-4454
chiprob@earthlink.net
mwinter@bflawfirm.com

Jay Barnes
BARNES & ASSOCIATES
219 East Dunklin St.
Jefferson City, MO 65101
jaybarnes5@zoho.com

Thomas Rosenfeld
GOLDENBERG HELLER ANTOGNOLI & ROWLAND PC
2227 South State Route 157
Edwardsville, IL 62025
618-656-5150
tom@ghalaw.com

Adam Voyles
LUBEL VOYLES LLP
5200 Montrose Blvd., Suite 800
Houston, TX 77086
713-284-5200
Adam@lubelvoyles.com

Douglas Campbell
Frederick Donald Rapone
CAMPBELL & LEVINE LLC
1700 Grant Building
Pittsburgh, PA 15219
(412) 261-0310
dac@camlev.com
fdr@camlev.com

Andrew Lyskowski
BERGMANIS LAW FIRM LLC
380 West US Highway 54, Suite 201
Camdenton, MO 65020
(573) 346-2111
alyskowski@ozarklawcenter.com

Mark C. Goldenberg
Kevin P. Green
GOLDENBERG HELLER ANTOGNOLI & ROWLAND PC
2227 South Route 157
P.O. Box 959
Edwardsville, IL 62025
(618)656-5150
kevin@ghalaw.com

CERTIFICATION OF BAR MEMBERSHIP

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

/s/ Barry R. Eichen
Barry R. Eichen
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
beichen@njadvocates.com

CERTIFICATION OF WORD COUNT

This brief complies with the type-volume limitation because this brief contains 6,999 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2010 in 14-point Times New Roman font.

/s/ Barry R. Eichen
Barry R. Eichen
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
beichen@njadvocates.com

CERTIFICATION OF SERVICE UPON COUNSEL

I hereby certify that on July 27, 2015, I electronically filed the foregoing using the Court's CM/ECF system, which sent a notification of such filing to all counsel of record.

Also, as per Fed. R. App. P. 25(a)(2)(B)(ii), I sent copies of the foregoing to the Office of the Clerk of Court and a copy to all Defendants counsel of record for delivery within 3 days.

/s/ Barry R. Eichen
Barry R. Eichen
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
beichen@njadvocates.com

CERTIFICATION OF IDENTICAL COMPLIANCE OF BRIEFS

I certify that the E-Brief and Hard Copies of the brief are identical.

/s/ Barry R. Eichen
Barry R. Eichen
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
beichen@njadvocates.com

CERTIFICATION OF VIRUS CHECK

I hereby certify that a virus check was performed on the E-Brief using Microsoft Security Essentials Version 1.197.699.0 and that no viruses were found.

/s/ Barry R. Eichen
Barry R. Eichen
EICHEN CRUTCHLOW ZASLOW & McELROY
40 Ethel Road
Edison, NJ 08817
Telephone: (732) 777-0100
beichen@njadvocates.com