PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

_____

No. 15-1441

_____

IN RE: NICKELODEON
CONSUMER PRIVACY LITIGATION

A.V.; C.A.F.; C.T.F.; M.P.; T.P.; K.T.; N.J.; T.M.;
STEPHANIE FRYAR,

Appellants

_____

On Appeal from the District Court
for the District of New Jersey
(Multidistrict Litigation No. 13-md-2443
District Court No. 2-12-cv-07829)
District Judge: Honorable Stanley R. Chesler

_____

Argued December 8, 2015

Before: FUENTES, SHWARTZ, and VAN ANTWERPEN,
Circuit Judges

(Opinion Filed: June 27, 2016)

Jason O. Barnes, Esq. **[ARGUED]**
Barnes & Associates
219 East Dunklin Street, Suite A
Jefferson City, MO 65101

Douglas A. Campbell, Esq.
Frederick D. Rapone, Esq.
Campbell & Levine, LLC
310 Grant Street, Suite 1700
Pittsburgh, PA 15219

Barry R. Eichen
Evan J. Rosenberg, Esq.
Eichen Crutchlow Zaslow & McElroy, LLP
40 Ethel Road
Edison, NJ 08817

James P. Frickleton, Esq.
Edward D. Robertson, III, Esq.
Bartimus Frickleton Robertson, P.C.
11150 Overbrook Road, Suite 200
Leawood, KS 66211

Edward D. Robertson, Jr., Esq.
Mary D. Winter, Esq.
Bartimus Frickleton Robertson, P.C.
715 Swifts Highway
Jefferson City, MO 65109

Mark C. Goldenberg, Esq.
Thomas Rosenfeld, Esq.
Goldenberg Heller Antognoli & Rowland, PC
2227 South State Route 157
Edwardsville, IL 62025

Adam Q. Voyles, Esq.
Lubel Voyles LLP
5020 Montrose Boulevard, Suite 800
Houston, TX 77006

Attorneys for Appellants

Alan J. Butler, Esq. **[ARGUED]**
Marc Rotenberg, Esq.
Electronic Privacy Information Center
1718 Connecticut Avenue, N.W., Suite 200
Washington, DC 20009

Attorneys for Amicus Curiae
Electronic Privacy Information Center

Jeremy Feigelson, Esq.
Debevoise & Plimpton LLP
919 Third Avenue
New York, NY 10022

David A. O'Neil, Esq. **[ARGUED]**
Debevoise & Plimpton LLP
801 Pennsylvania Avenue, N.W., Suite 500
Washington, DC 20004

Seth J. Lapidow, Esq.
Stephen M. Orlofsky, Esq.
Blank Rome LLP
301 Carnegie Center, Third Floor
Princeton, NJ 08540

Attorneys for Appellee Viacom, Inc.

Colleen Bal, Esq.
Michael H. Rubin, Esq. **[ARGUED]**
Wilson, Sonsini, Goodrich & Rosati, PC
One Market Street
Spear Tower, Suite 3300
San Francisco, CA 94105

Tonia O. Klausner, Esq.
Wilson Sonsini Goodrich & Rosati, PC
1301 Avenue of the Americas, 40th Floor
New York, NY 10019

Jeffrey J. Greenbaum, Esq.
Joshua N. Howley, Esq.
Sills, Cummis & Gross P.C.
One Riverfront Plaza
Newark, NJ 07102

Attorneys for Appellee Google, Inc.

Jeffrey B. Wall, Esq. **[ARGUED]**
Sullivan & Cromwell LLP
1700 New York Avenue, N.W., Suite 700
Washington, DC 20006

Attorney for Amicus Curiae
Chamber of Commerce of the United States of America

OPINION OF THE COURT

FUENTES, *Circuit Judge*:

Table of Contents

Most of us understand that what we do on the Internet is not completely private. How could it be? We ask large companies to manage our email, we download directions from smartphones that can pinpoint our GPS coordinates, and we look for information online by typing our queries into search engines. We recognize, even if only intuitively, that our data has to be going somewhere. And indeed it does, feeding an entire system of trackers, cookies, and algorithms designed to capture and monetize the information we generate. Most of the time, we never think about this. We browse the Internet, and the data-collecting infrastructure of the digital world hums along quietly in the background.

Even so, not everything about our online behavior is necessarily public. Numerous federal and state laws prohibit certain kinds of disclosures, and private companies often promise to protect their customers' privacy in ways that may be enforceable in court. One of our decisions last year, *In re Google Inc. Cookie Placement Consumer Privacy Litigation*,[1] addressed many of these issues. This case addresses still more.

This is a multidistrict consolidated class action. The plaintiffs are children younger than 13 who allege that the defendants, Viacom and Google, unlawfully collected personal information about them on the Internet, including what webpages they visited and what videos they watched on Viacom's websites. Many of the plaintiffs' claims overlap substantially with those we addressed in *Google*, and indeed fail for similar reasons. Even so, two of the plaintiffs' claims—one for violation of the federal Video Privacy Protection Act, and one for invasion of privacy under New Jersey law—raise questions of first impression in our Circuit.

The Video Privacy Protection Act, passed by Congress in 1988, prohibits the disclosure of personally identifying information relating to viewers' consumption of video-related services. Interpreting the Act for the first time, we hold that the law permits plaintiffs to sue only a person who *discloses* such information, not a person who *receives* such information. We also hold that the Act's prohibition on the disclosure of personally identifiable information applies only to the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior. In

[1] 806 F.3d 125 (3d Cir. 2015).

our view, the kinds of disclosures at issue here, involving digital identifiers like IP addresses, fall outside the Act's protections.

The plaintiffs also claim that Viacom and Google invaded their privacy by committing the tort of intrusion upon seclusion. That claim arises from allegations that Viacom explicitly promised not to collect any personal information about children who browsed its websites and then, despite its assurances, did exactly that. We faced a similar allegation of deceitful conduct in *Google*, where we vacated the dismissal of state-law claims for invasion of privacy and remanded them for further proceedings. We reach a similar result here, concluding that, at least as to Viacom, the plaintiffs have adequately alleged a claim for intrusion upon seclusion. In so doing, we hold that the 1998 Children's Online Privacy Protection Act, a federal statute that empowers the Federal Trade Commission to regulate websites that target children, does not preempt the plaintiffs' state-law privacy claim.

Accordingly, we will affirm the District Court's dismissal of most of the plaintiffs' claims, vacate its dismissal of the claim for intrusion upon seclusion against Viacom, and remand the case for further proceedings.

I. Background

We begin by summarizing the allegations in the plaintiffs' complaints.[2]

[2] The plaintiffs filed a Master Consolidated Class Action Complaint that included seven claims. (*See* App. Vol. II at

A. Internet Cookie Technology

When a person uses a web browser to access a website, the browser sends a "GET" request to the server hosting that site. So, for example, if a person types "www.nick.com" into the address bar of his or her web browser, the browser contacts the server where Nick.com is hosted and transmits data back to the user's computer.[3] In addition to other content, Nick.com may also display ads from third parties. These ads typically reside on a different server. To display the ad, the Nick.com server will direct the user's browser to send another "GET" request to the third-party server, which will then transmit the ad directly to the user's computer. From the user's perspective, all of this appears to happen simultaneously, and all the visual information on Nick.com appears to originate from a single source. In reality, the Nick.com website is an assemblage of content from multiple

---

59–107.) The District Court dismissed four claims with prejudice, two claims without prejudice as to both defendants, and one claim with prejudice as to Google but without prejudice as to Viacom. The plaintiffs then filed a Second Consolidated Class Action Complaint. (*See id.* at 108–62.) The two complaints are cited throughout as the "First Compl." and "Second Compl." As this is "an appeal from a Rule 12(b)(6) dismissal, we must accept all well-pled allegations in the complaint as true and draw all reasonable inferences in favor of the non-moving party." *Brown v. Card Serv. Ctr.*, 464 F.3d 450, 452 (3d Cir. 2006).

[3] Second Compl. ¶¶ 25–26.

servers hosted by different parties.[4]

An Internet "cookie" is a small text file that a web server places on a user's computing device.[5] Cookies allow a website to "remember" information about a user's browsing activities (such as whether or not the user is logged-in, or what specific pages the user has visited). We can distinguish between first-party cookies, which are injected into a user's computer by a website that the user chooses to visit (*e.g.*, Nick.com), and third-party cookies, which are placed on a user's computer by a server other than the one that a person intends to visit (*e.g.*, by an ad company like Google).[6]

Advertising companies use third-party cookies to help them target advertisements more effectively at customers who might be interested in buying a particular product. Cookies are particularly powerful if the same company hosts ads on more than one website. In those circumstances, advertising companies are able to follow a user's browsing habits across multiple websites that host the company's ads. Given Google's dominance in the Internet advertising market, the plaintiffs claim that Google is able to use cookies to track users' behavior across large swaths of the Internet.[7]

---

[4] *Id.* ¶¶ 27–29.

[5] *Id.* ¶ 31.

[6] *Id.* ¶ 33.

[7] *Id.* ¶ 45.

B. Factual Allegations

Defendant Viacom owns the children's television station Nickelodeon. It also operates Nick.com, a website geared towards children that offers streaming videos and interactive games.[8] A child registers to use Nick.com by signing up for an account and choosing a username and password.[9] During the registration process, a child provides his or her birthdate and gender to Viacom, and Viacom then assigns the child a code based on that information.[10] The plaintiffs also assert that Viacom's registration form includes a message to children's parents: "HEY GROWN-UPS: We don't collect ANY personal information about your kids. Which means we couldn't share it even if we wanted to!"[11]

The plaintiffs allege that Viacom and Google unlawfully used cookies to track children's web browsing and video-watching habits on Viacom's websites. They claim that

---

[8] *Id.* ¶¶ 1, 101, 109. The plaintiffs' first complaint also raised allegations relating to NickJr.com and NeoPets.com, but those websites do not appear in the plaintiffs' second complaint. *See* First Compl. ¶¶ 1, 126.

[9] Second Compl. ¶¶ 102–03.

[10] Viacom apparently refers to these as "rugrat codes," with the moniker "rugrat" coming from the long-running Nickelodeon cartoon of the same name. So, for example, the "rugrat code" for all six-year-old boys registered to use Viacom's websites is "Dil," the name of one of the *Rugrats* characters. *Id.* ¶¶ 104, 111–12.

[11] *Id.* ¶ 103.

the defendants collected information about children in at least four ways.

First, when a user visits one of Viacom's websites, Viacom places its own first-party cookie on that user's computer.[12] This permits Viacom to track a child's behavior, including which games a child plays and which videos a child watches.

Second, Google contracts with Viacom to place advertisements on Viacom's websites. As a result, Google is able to place third-party cookies on the computers of persons who visit those websites, including children.[13]

Third, the plaintiffs claim that, "[u]pon information and belief, Viacom also provided Google with access to the profile and other information contained within Viacom's first-party cookies."[14]

Fourth, the plaintiffs assert that, once Google places a cookie on a person's computer, it can track that person across any website on which Google displays ads.[15] Google uses so-called "Doubleclick.net cookies" to accomplish this task.[16] In addition, Google offers its own collection of online services

---

[12] *Id.* ¶ 67.

[13] *Id.* ¶ 68.

[14] *Id.* ¶ 70.

[15] *Id.* ¶¶ 79–87.

[16] *Id.* ¶ 78.

to Google account-holders and other web users, including Gmail, Google Maps, and YouTube (which Google owns).[17] The plaintiffs claim that Google combines information that it collects from people using *its* websites with information it gleans from displaying ads on *others'* websites.[18] They also claim that "Viacom is aware of Google's ubiquitous presence on the Internet and its tracking of users."[19]

In the aggregate, the plaintiffs claim that Viacom discloses to Google, and Google collects and tracks, all of the following information about children who visit Viacom's websites:

> (1) the child's username/alias; (2) the child's gender; (3) the child's birthdate; (4) the child's IP address; (5) the child's browser settings; (6) the child's unique device identifier; (7) the child's operating system; (8) the child's screen resolution; (9) the child's browser version; (10) the child's web communications, including but not limited to detailed URL requests and video materials requested and obtained from

---

[17] *Id.* ¶ 80.

[18] *Id.* ¶¶ 64, 83; *see also* First Compl. ¶ 155 ("Upon information and belief, in addition to intercepting the Plaintiffs' communications with the Viacom children's websites, Google used the cookies to track the Plaintiffs' communications with other websites on which Google places advertisements and related tracking cookies . . . .").

[19] Second Compl. ¶ 93.

> Viacom's children's websites; and (11) the DoubleClick persistent cookie identifiers.[20]

The purpose of all of this information gathering is to sell targeted advertising based on users' web browsing. In fact, the plaintiffs claim that targeting advertisements to children is more profitable than targeting advertising to adults "because children are generally unable to distinguish between content and advertisements."[21] They cite a *Wall Street Journal* article stating that "popular children's websites install more tracking technologies on personal computers than do the top websites aimed at adults."[22]

The plaintiffs also allege a number of facts about online tracking more generally. They claim that it is surprisingly easy for advertising companies to identify web users' offline identities based on their online browsing habits. They cite a Stanford professor, Arvind Narayanan, for the proposition that "re-identification" of web users based on seemingly anonymous data is possible based on users' commercial transactions, web browsing, search histories, and other factors.[23] The plaintiffs also claim that companies can use "browser fingerprinting" to identify website visitors based on the configuration of a user's browser and operating

---

[20] *Id.* ¶ 76.

[21] *Id.* ¶ 55.

[22] *Id.* ¶ 56 (quoting Steve Stecklow, *On the Web, Children Face Intensive Tracking*, Wall St. J., Sept. 17, 2010).

[23] *Id.* ¶¶ 57–58.

system.[24] Using these techniques, the plaintiffs claim that Google and Viacom "are able to link online and offline activity and identify specific users, including the Plaintiffs and children that form the putative class."[25]

Lastly, the plaintiffs allege a number of facts in order to demonstrate that the defendants' behavior violated contemporary social norms. To that end, they claim that Google is a member of an organization called the Interactive Advertising Bureau that promulgates a Code of Conduct for its members. That Code is said to prohibit members from collecting "personal information" from children "they have actual knowledge are under the age of 13."[26] The plaintiffs also cite a survey of more than 2,000 adults conducted by the Center for Digital Democracy. According to the survey, 80 percent of respondents oppose the tracking of children even where an advertiser does not "know a child's name and address," and 91 percent believe advertisers should receive a parent's permission before placing tracking software on a minor child's computing device.[27]

C. Procedural History in the District Court

In June of 2013, the Judicial Panel on Multidistrict Litigation transferred six privacy-related suits against Viacom

---

[24] *Id.* ¶¶ 61–62.

[25] *Id.* ¶ 64.

[26] *Id.* ¶ 137(b).

[27] *Id.* ¶ 164(c), (d).

and Google to the District of New Jersey for consolidation.[28] The plaintiffs in these cases seek to represent two classes. The first is a class of "[a]ll children under the age of 13 in the United States who visited the website Nick.com and had Internet cookies that tracked their communications placed on their computing devices by Viacom and Google."[29] The second is a class of "[a]ll children under the age of 13 in the United States who were registered users of Nick.com and who engaged with one or more video materials on such site, and who had their video viewing histories knowingly disclosed by Viacom to Google."[30] The proposed classes are not bounded by any time period, although the plaintiffs do note that Viacom "revamped its Nick.com website" in August of 2014 so that it "no longer discloses the particular video viewing or game histories of individual users of Nick.com to Google."[31]

Shortly after transfer to the District of New Jersey, the plaintiffs filed their first consolidated complaint. It raised six

[28] *In re Nickelodeon Consumer Privacy Litig.*, 949 F. Supp. 2d 1377 (J.P.M.L. 2013).

[29] Second Compl. ¶ 115.

[30] *Id.*

[31] *Id.* ¶ 101.

claims, including violations of (i) the Wiretap Act,[32] (ii) the Stored Communications Act,[33] (iii) the California Invasion of Privacy Act,[34] (iv) the Video Privacy Protection Act,[35] (v) the New Jersey Computer Related Offenses Act,[36] and (vi) a claim under New Jersey common law for intrusion upon seclusion.

The District Court granted the defendants' motion to dismiss all of the plaintiffs' claims, three of them with

---

[32] 18 U.S.C. § 2510, *et seq.* The Wiretap Act, "formally known as the 1968 Omnibus Crime Control and Safe Streets Act," was technically superseded by the Electronic Communications Privacy Act in 1986. *Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 113 & n.7 (3d Cir. 2003), *as amended* (Jan. 20, 2004). We refer to the Wiretap Act throughout, as we did in *Google*.

[33] 18 U.S.C. § 2701, *et seq.*

[34] Cal. Penal Code § 630, *et seq.*

[35] 18 U.S.C. § 2710.

[36] N.J. Stat. Ann. § 2A:38A–3. The plaintiffs' first complaint also included a count alleging unjust enrichment. (*See* First Compl. ¶¶ 198–201.) The District Court dismissed this claim with prejudice. (*See* App. Vol. I at 43–44.) The plaintiffs eventually explained that they sought to use unjust enrichment "not as an independent action in tort, but as a measure of damages under the [New Jersey Computer Related Offenses Act] in a quasi-contractual sense." (Pls. Br. at 47.)

prejudice.[37] The District Court nonetheless permitted the plaintiffs to file an amended complaint revising their claims under the Video Privacy Protection Act, the New Jersey Computer Related Offenses Act, and for intrusion upon seclusion. The plaintiffs did so, the defendants again moved to dismiss, and the District Court dismissed the case in its entirety.[38] The plaintiffs now appeal.[39]

Our Court's review of a decision dismissing a

---

[37] *In re Nickelodeon Consumer Privacy Litig.*, No. 12-cv-7829 (SRC), 2014 WL 3012873, at *20 (D.N.J. July 2, 2014) ("*Nickelodeon I*"). The District Court dismissed the unjust enrichment claim with prejudice, but, as explained earlier, that was never a standalone cause of action. It also dismissed the plaintiffs' Video Privacy Protection Act claims against Google with prejudice, but allowed the plaintiffs to amend their Video Privacy claim against Viacom. *Id.*

[38] *In re Nickelodeon Consumer Privacy Litig.*, No. 12-cv-7829 (SRC), 2015 WL 248334, at *7 (D.N.J. Jan. 20, 2015) ("*Nickelodeon II*").

[39] This is a diversity suit brought by plaintiffs under the Class Action Fairness Act and various provisions of federal law. *See* 28 U.S.C. §§ 1332(d)(2), 1331. The District Court exercised supplemental jurisdiction over plaintiffs' state-law claims under 28 U.S.C. § 1367. The District Court entered an order dismissing the case on January 20, 2015, and the plaintiffs filed a timely notice of appeal. (App. Vol. I at 1, 58.) This Court has appellate jurisdiction over the final order of the District Court under 28 U.S.C. § 1291.

complaint is plenary.[40]

II. Arguments and Claims Foreclosed by Our Decision in *Google*

Google came down in November of 2015, several months after briefing in this case was complete but before oral argument. We therefore asked the parties to submit their views about *Google*'s effect on the present litigation. As will become clear, we conclude that *Google* is fatal to several of the plaintiffs' claims.

The *Google* plaintiffs consisted of a class of persons who used two web browsers: Apple's Safari and Microsoft's Internet Explorer.[41] These browsers came with cookie-blocking options designed to protect users' privacy while they browsed the Internet. In February of 2012, a Stanford graduate student revealed that Google and several other advertising companies had devised ways to evade these cookie-blocking options, even while touting publicly that they respected their users' choices about whether to take advantage of cookie-blocking technology.[42]

The *Google* plaintiffs then filed a federal lawsuit alleging violations of the Wiretap Act, the Stored Communications Act, and the Computer Fraud and Abuse

---

[40] *Finkelman v. Nat'l Football League*, 810 F.3d 187, 192 (3d Cir. 2016).

[41] *Google*, 806 F.3d at 133.

[42] *Id.* at 132.

Act.[43] They also brought claims for violation of the California Invasion of Privacy Act and for intrusion upon seclusion and invasion of privacy under California law.[44]

The district court dismissed those claims in their entirety.[45] We affirmed the dismissals of all claims except those for invasion of privacy and intrusion upon seclusion. With respect to those claims, we determined that "[a] reasonable factfinder could conclude that the means by which defendants allegedly accomplished their tracking, i.e., by way of a deceitful override of the plaintiffs' cookie blockers, marks the serious invasion of privacy contemplated by California law."[46]

With this background in mind, we turn to *Google*'s effect on the present litigation.

A. Article III Standing

"To establish Article III standing, a plaintiff must demonstrate '(1) an injury-in-fact, (2) a sufficient causal

---

[43] *Id.* at 133.

[44] The *Google* plaintiffs brought other statutory claims not relevant to this case, including claims for alleged violations of California's Unfair Competition Law, its Comprehensive Computer Data Access and Fraud Act, and its Consumers Legal Remedies Act. *See id.*

[45] *See In re Google Inc. Cookie Placement Consumer Privacy Litig.*, 988 F. Supp. 2d 434 (D. Del. 2013).

[46] *Google*, 806 F.3d at 153.

connection between the injury and the conduct complained of, and (3) a likelihood that the injury will be redressed by a favorable decision.'"[47] To allege an injury-in-fact, "a plaintiff must claim 'the invasion of a concrete and particularized legally protected interest' resulting in harm 'that is actual or imminent, not conjectural or hypothetical.'"[48] A harm is "particularized" if it "affect[s] the plaintiff in a personal and individual way."[49] It is "concrete" if it is "'*de facto*'; that is, it must actually exist" rather than being only "abstract."[50]

The defendants assert that Article III standing is lacking in this case because the disclosure of information about the plaintiffs' online activities does not qualify as an injury-in-fact. *Google* rejected a similar argument, stating that, when it comes to laws that protect privacy, a focus on "economic loss is misplaced."[51] Instead, in some cases an injury-in-fact "may exist solely by virtue of statutes creating legal rights, the invasion of which creates standing."[52]

---

[47] *Finkelman*, 810 F.3d at 193 (quoting *Neale v. Volvo Cars of N. Am., LLC*, 794 F.3d 353, 358–59 (3d Cir. 2015) (internal quotation marks omitted and punctuation modified)).

[48] *Id.* (quoting *Blunt v. Lower Merion Sch. Dist.*, 767 F.3d 247, 278 (3d Cir. 2014)).

[49] *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 n.1 (1992).

[50] *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016).

[51] *Google*, 806 F.3d at 134.

[52] *Id.* (quoting *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 373 (1982)).

Applying this principle, other courts have found standing in cases arising from allegedly unlawful disclosures similar to those at issue here.[53]

The Supreme Court's recent decision in *Spokeo, Inc. v. Robins*[54] does not alter our prior analysis in *Google*. The plaintiff there alleged that Spokeo, an online background check company, reported inaccurate information about him to its customers. The plaintiff then sued Spokeo under the Fair Credit Reporting Act. The Ninth Circuit concluded that the plaintiff's "personal interests in the handling of his credit information," coupled with the purported "violations of statutory rights created by the [Act]," were sufficient to satisfy the injury-in-fact requirement of Article III standing.[55] The Supreme Court granted certiorari in *Spokeo* to address the question of "[w]hether Congress may confer Article III standing upon a plaintiff who suffers no concrete harm, and who therefore could not otherwise invoke the jurisdiction of a federal court, by authorizing a private right of action based on

---

[53] *See, e.g.*, *Sterk v. Redbox Automated Retail, LLC*, 770 F.3d 618, 623 (7th Cir. 2014) ("By alleging that Redbox disclosed their personal information in violation of the [Video Privacy Protection Act], [plaintiffs] have met their burden of demonstrating that they suffered an injury in fact that success in this suit would redress.").

[54] 136 S. Ct. 1540.

[55] *See Robins v. Spokeo, Inc.*, 742 F.3d 409, 413 (9th Cir. 2014).

a bare violation of a federal statute."[56] Rather than answer that question directly, the Supreme Court vacated the judgment of the Ninth Circuit and remanded the case for further proceedings.

In doing so, the Supreme Court explained that the Ninth Circuit erred in its standing analysis by focusing only on whether the plaintiff's purported injury was "particularized" without also assessing whether it was sufficiently "concrete."[57] In reaching this conclusion, the Court noted that even certain kinds of "intangible" harms can be "concrete" for purposes of Article III. When evaluating whether such a harm qualifies as an injury-in-fact, judges should consider whether the purported injury "has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts."[58] Congress's judgment on such matters is "also instructive and important," meaning that Congress may "elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law."[59]

---

[56] Supreme Court, No. 13-1339, Question Presented, http://www.supremecourt.gov/qp/13-01339qp.pdf (last visited June 14, 2016).

[57] *Spokeo*, 136 S. Ct. at 1550 ("Because the Ninth Circuit failed to fully appreciate the distinction between concreteness and particularization, its standing analysis was incomplete.").

[58] *Id.* at 1549.

[59] *Id.* (alteration in original) (quoting *Lujan*, 504 U.S. at 578).

Intangible harms that may give rise to standing also include harms that "may be difficult to prove or measure," such as unlawful denial of access to information subject to disclosure.[60] What a plaintiff cannot do, according to the Court, is treat a "bare procedural violation . . . [that] may result in no harm" as an Article III injury-in-fact.[61] The Court provided two examples, including a defendant's failure to comply with a statutory notice requirement and, in the context of the Fair Credit Reporting Act, the dissemination of inaccurate information about a plaintiff, such as an incorrect zip code, that does not "cause harm or present any material risk of harm."[62]

None of these pronouncements calls into question whether the plaintiffs in this case have Article III standing. The purported injury here is clearly particularized, as each plaintiff complains about the disclosure of information relating to his or her online behavior. While perhaps "intangible," the harm is also concrete in the sense that it involves a clear *de facto* injury, *i.e.*, the unlawful disclosure of legally protected information. Insofar as *Spokeo* directs us to consider whether an alleged injury-in-fact "has traditionally been regarded as providing a basis for a lawsuit,"[63] *Google* noted that Congress has long provided plaintiffs with the right

---

[60] *Id.* at 1549–50 (citing *Fed. Election Comm'n v. Akins*, 524 U.S. 11 (1998), and *Pub. Citizen v. Dep't of Justice*, 491 U.S. 440 (1989)).

[61] *Id.* at 1550.

[62] *Id.*

[63] *Id.* at 1549.

to seek redress for unauthorized disclosures of information that, in Congress's judgment, ought to remain private.[64]

Accordingly, we conclude that the plaintiffs have alleged facts which, if true, are sufficient to establish Article III standing.

B. The Federal Wiretap Act

The plaintiffs bring a claim against both Viacom and Google under the federal Wiretap Act. A plaintiff pleads a *prima facie* case under the Wiretap Act by showing that the defendant "(1) intentionally (2) intercepted, endeavored to intercept or procured another person to intercept or endeavor to intercept (3) the contents of (4) an electronic communication, (5) using a device."[65]

The District Court rejected the plaintiffs' wiretapping claim for two reasons. First, it concluded that Google's conduct was not unlawful in view of how Google allegedly communicated with the plaintiffs' computers. The Wiretap Act does not make it unlawful "for a person to 'intercept . . . electronic communication' if the person 'is [1] a party to the communication or [2] where one of the parties to the communication has given prior consent to such

---

[64] *See Google*, 806 F.3d at 134 & n.19 (citing *Doe v. Chao*, 540 U.S. 614, 641 (2004) (Ginsburg, J., dissenting) (discussing standing under the Privacy Act of 1974)).

[65] *Id.* at 135 (quoting *In re Pharmatrak, Inc. Privacy Litig.*, 329 F.3d 9, 18 (1st Cir. 2003)).

interception . . . .'"[66] Here, Google was either a party to all communications with the plaintiffs' computers or was permitted to communicate with the plaintiffs' computers by Viacom, who was itself a party to all such communications. Accordingly, the plaintiffs failed to state a legally sufficient wiretapping claim.

Second, the District Court concluded that the information Google allegedly intercepted was not of the kind protected by the statute. The Wiretap Act prohibits "intercept[ion]" of "any wire, oral, or electronic communication," and defines "intercept[ion]" as "the aural or other acquisition of the contents of any wire, electronic, or oral communication through the use of any electronic, mechanical, or other device."[67] The plaintiffs alleged that, insofar as Viacom permitted Google to access URLs that revealed which videos a child watched, such as "http://www.nick.com/shows/penguins-of-madagascar,"[68] Google intercepted the "contents" of the plaintiffs' communications. The District Court disagreed. It concluded that a URL is more akin to a telephone number (whose interception cannot support a Wiretap Act claim) than a substantive conversation (whose interception can give rise to

[66] *Nickelodeon I*, 2014 WL 3012873, at *13 (quoting 18 U.S.C. § 2511(d)(2)).

[67] 18 U.S.C. §§ 2511(1)(a), 2510(4).

[68] First Compl. ¶¶ 78, 140.

such a claim).[69] The District Court dismissed the plaintiffs' Wiretap Act claim on this ground as well.[70]

Google vindicated the District Court's reasoning as to one-party consent, but not with respect to the definition of "contents." We there concluded that companies that place cookies on a computing device are, at least on facts analogous to those alleged here, "parties to any communications that they acquired," meaning that such companies are not liable under the Wiretap Act.[71] We also concluded that "some queried URLs qualify as content,"[72] reasoning that a URL may convey "substantive information" about web browsing activity instead of mere "dialing, routing, addressing, or

---

[69] *Compare Smith v. Maryland*, 442 U.S. 735, 741 (1979) (explaining that pen registers "disclose only the telephone numbers that have been dialed—a means of establishing communication," and not "any communication between the caller and the recipient of the call" (quoting *United States v. N.Y. Tel. Co.*, 434 U.S. 159, 167 (1977))), *with Katz v. United States*, 389 U.S. 347, 357–58 (1967) (holding that warrantless wiretapping of a telephone call violates the Fourth Amendment).

[70] *Nickelodeon I*, 2014 WL 3012873, at *14–15.

[71] *Google*, 806 F.3d at 145.

[72] *Id.* at 139 ("[T]he domain name portion of the URL—everything before the '.com'—instructs a centralized web server to direct the user to a particular website, but post-domain name portions of the URL are designed to communicate to the visited website which webpage content to send the user.").

signaling information."[73] The first holding is fatal to the plaintiffs' claim.

The plaintiffs try to resist this conclusion. They contend that the one-party consent language in the Wiretap Act does not apply here because the plaintiffs were minors who were incapable of consenting at all. We agree with the District Court that the plaintiffs "have cited no authority for the proposition that the Wiretap Act's one-party consent regime depends on the age of the non-consenting party."[74] Given the vast potential for unexpected liability whenever a minor happened to browse an Internet site that deployed cookies, we decline to adopt such a reading of the Act here.[75]

The plaintiffs also argue that, even if Google and Viacom were parties to any intercepted communications, they nonetheless acted unlawfully because the Wiretap Act imposes liability whenever someone intercepts information "for the purpose of committing . . . [a] tortious act."[76] Here, the plaintiffs allege that the defendants' use of cookies amounted to the common law tort of intrusion upon seclusion. We rejected a similar argument in *Google*, reasoning that the "tortious act" provision of the wiretapping statute only applies

---

[73] *Id.* at 137.

[74] *Nickelodeon I*, 2014 WL 3012873, at *14.

[75] In addition, adopting the plaintiffs' view could mean that the alleged inability of a minor to consent would vitiate another party's consent, which we conclude would be inconsistent with the Wiretap Act's statutory language.

[76] 18 U.S.C. § 2511(2)(d).

when "the offender intercepted the communication for the purpose of a tortious or criminal act that is *independent* of the intentional act of recording."[77] Consistent with our reasoning in *Google*, we will affirm the District Court's dismissal of the plaintiffs' wiretapping claim.[78]

C. The California Invasion of Privacy Act

The California Invasion of Privacy Act "broadly prohibits the interception of wire communications and disclosure of the contents of such intercepted communications."[79] *Google* affirmed the dismissal of a claim

---

[77] *Google*, 806 F.3d at 145 (quoting *Caro v. Weintraub*, 618 F.3d 94, 100 (2d Cir. 2010)).

[78] The Wiretap Act also makes it unlawful for a person to "intentionally . . . procure[] any other person to intercept or endeavor to intercept, any wire, oral, or electronic communications." 18 U.S.C. § 2511(1)(a). The plaintiffs broadly assert that "Viacom procured Google to intercept the content of the Plaintiffs' communications with other websites, and, upon information and belief, profited from Google's unauthorized tracking on other sites . . . ." (Pls. Br. at 8.) The plaintiffs' allegations of procurement in this case are entirely conclusory and therefore fail to comport with "the Supreme Court's teaching that all aspects of a complaint must rest on 'well-pleaded factual allegations' and not 'mere conclusory statements.'" *Finkelman*, 810 F.3d at 194 (quoting *Ashcroft v. Iqbal*, 556 U.S. 662, 678–79 (2009)).

[79] *Google*, 806 F.3d at 152 (quoting *Tavernetti v. Superior Court*, 583 P.2d 737, 739 (Cal. 1978)).

under the California Act on the view that, like the federal wiretapping statute, the California Act does not apply when the alleged interceptor was a party to the communications.[80] For the same reason, we will affirm the District Court's dismissal of the plaintiffs' similar claim here.[81]

D. The Federal Stored Communications Act

Passed in 1986, the Stored Communications Act aims to prevent "potential intrusions on individual privacy arising from illicit access to 'stored communications in remote computing operations and large data banks that stored e-mails.'"[82] A person violates the Stored Communications Act

---

[80] *Id.* (stating that the California Invasion of Privacy Act "is aimed only at 'eavesdropping, or the secret monitoring of conversations by third parties'" (quoting *Ribas v. Clark*, 696 P.2d 637, 640 (Cal. 1985) (in bank))).

[81] In their submission regarding *Google*'s application to the present case, the plaintiffs argue that the defendants also may be liable under § 632 of the California Invasion of Privacy Act, which prohibits eavesdropping on or recording confidential communications. The plaintiffs did not discuss § 632 in their complaints, nor did they brief its application before us. Accordingly, any arguments based on § 632 are now waived. *See Harris v. City of Philadelphia*, 35 F.3d 840, 845 (3d Cir. 1994) ("This court has consistently held that it will not consider issues that are raised for the first time on appeal.").

[82] *Google*, 806 F.3d at 145 (quoting *Garcia v. City of Laredo, Tex.*, 702 F.3d 788, 791 (5th Cir. 2012)).

whenever he or she "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system."[83]

In *Google*, we affirmed dismissal of a claim under the Stored Communications Act because, in our view, personal computing devices were not protected "facilities" under the statute.[84] For the same reason, we will affirm dismissal of the plaintiffs' Stored Communications Act claim here.[85]

---

[83] *Id.* at 145–46 (quoting 18 U.S.C. § 2701(a)).

[84] *Id.* at 148.

[85] The plaintiffs argue that, even if *Google* stated that "a personal computing device" is not a protected facility under the Stored Communications Act, it did not go so far as to hold that a personal web browser is not a protected facility. *See* Ltr. from J. Frickleton to Ct. at 4 (Nov. 24, 2015). This argument parses the language of *Google* too finely. *Google* explained that "[t]he origin of the Stored Communications Act confirms that Congress crafted the statute to specifically protect information held by centralized communication providers." 806 F.3d at 147. Since neither a personal computing device nor a personal web browser is akin to a "centralized communication provider," the plaintiffs' proposed distinction does not salvage their claim. *See ACTV, Inc. v. Walt Disney Co.*, 204 F. Supp. 2d 650, 656 (S.D.N.Y. 2002) (defining "web browser" as "a software application that

E. The New Jersey Computer Related Offenses Act

The New Jersey Computer Related Offenses Act makes it unlawful to alter, damage, access, or obtain data from a computer without authorization.[86] It also permits "[a] person or enterprise damaged in business or property" to sue for compensatory and punitive damages, as well as fees and costs.[87] The plaintiffs allege that Viacom and Google violated the New Jersey Act by using Internet cookies to "access[] Plaintiffs' and Class Members' computers in order to illegally harvest Plaintiffs' and Class Members' personal information" without their consent.[88]

The District Court dismissed this claim because, in its view, the plaintiffs failed to allege that they had been "damaged in business or property," as the plain text of the New Jersey Act requires. The plaintiffs believe that the District Court erred by failing to credit their theory of damage—namely, that the defendants' appropriation of their personal information, without compensation, constituted

---

can be used to locate and display web pages in human-readable form"); *New York v. Microsoft Corp.*, 224 F. Supp. 2d 76, 245–46 (D.D.C. 2002) ("[A] web browser provides the ability for the end user to select, retrieve, and perceive resources on the Web.").

[86] N.J. Stat. Ann. 2A:38A–3.

[87] *Id.*

[88] Second Compl. ¶ 153.

unjust enrichment. The plaintiffs concede that "unjust enrichment has never been used as a measure of damages" under the New Jersey Act, but nonetheless encourage us to embrace this novel theory now.[89] We decline to do so.

In the first place, we have previously said that a claim under the New Jersey Act "require[s] proof of some activity vis-à-vis the information other than simply gaining access to it,"[90] and the plaintiffs allege the defendants did no more than "gain access" to their information here. In addition, crediting this novel theory of injury would be inconsistent with our treatment of similar allegations in *Google*. The plaintiffs there brought claims for violation of the federal Computer Fraud and Abuse Act,[91] which, like the New Jersey Act, requires a private plaintiff to show proof of "damage or loss."[92] The *Google* plaintiffs failed to satisfy this requirement because they "allege[d] no facts suggesting that they ever participated or intended to participate in the market [for sale of their information], or that the defendants prevented them from capturing the full value of their internet usage information for themselves."[93] Nor did they ever assert that "they sought to monetize information about their internet usage, nor that they ever stored their information with a future

---

[89] Pls. Reply Br. at 25.

[90] *P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore, LLC*, 428 F.3d 504, 509 (3d Cir. 2005).

[91] 18 U.S.C. § 1030.

[92] *Id.* § 1030(g).

[93] *Google*, 806 F.3d at 149.

sale in mind."[94]

The plaintiffs' claim here fails for the same reason. To be sure, the New Jersey courts are free to interpret the requirement to show "damage[] in business or property" under the New Jersey Act differently than federal courts interpret the analogous requirement in the Computer Fraud and Abuse Act. But the plaintiffs have pointed us to no authority indicating that federal and state courts understand the two laws differently. In fact, the opposite appears to be true: courts seem to have interpreted the New Jersey Act in harmony with its federal counterpart.[95]

Because we conclude that the plaintiffs have failed to allege the kind of injury that the New Jersey Act requires, we will affirm the District Court's dismissal of their claim.

III. Claims Raising Issues Beyond Those We Addressed in *Google*

While our spadework in *Google* goes a long way towards resolving this case, it does not do so entirely. The plaintiffs bring two claims—one for violation of the Video Privacy Protection Act, and one for intrusion upon seclusion under New Jersey law—that require us to break new ground.

---

[94] *Id.*

[95] *See, e.g.*, *Mu Sigma, Inc. v. Affine, Inc.*, No. 12-cv-1323 (FLW), 2013 WL 3772724, at *9–10 (D.N.J. July 17, 2013) (dismissing claims under the state and federal computer statutes for identical reasons).

A. The Video Privacy Protection Act

Congress passed the Video Privacy Protection Act in 1988 after the *Washington City Paper* published Supreme Court nominee Robert Bork's video rental history.[96] "The paper had obtained (without Judge Bork's knowledge or consent) a list of the 146 films that the Bork family had rented from a Washington, D.C.-area video store."[97] According to the Senate Report accompanying the law's passage, Congress passed the Act "[t]o preserve personal privacy with respect to the rental, purchase or delivery of video tapes or similar audio visual materials."[98]

The Act creates a private cause of action for plaintiffs to sue persons who disclose information about their video-watching habits. Unfortunately, as the Seventh Circuit has noted, the Act "is not well drafted,"[99] requiring us to begin by summarizing a bit of legislative jargon. The Act defines several key terms:

---

[96] *See* S. Rep. No. 100-599, at 5 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342-1 ("Senate Report"), *also available at* 1988 WL 243503.

[97] *Mollett v. Netflix, Inc.*, 795 F.3d 1062, 1065 (9th Cir. 2015).

[98] Senate Report at 1.

[99] *Sterk v. Redbox Automated Retail, LLC*, 672 F.3d 535, 538 (7th Cir. 2012).

- **Consumer:** "any renter, purchaser, or subscriber of goods or services from a video tape service provider."[100]

- **Video tape service provider:** "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials."[101]

- **Personally identifiable information:** "includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."[102]

To state a claim under the Act, a plaintiff must allege that "[a] video tape service provider . . . knowingly disclose[d], to any person, personally identifiable information concerning any consumer of such provider."[103] The Act (i) sets a minimum penalty of $2,500 per violation, (ii) permits a plaintiff to recover punitive damages, reasonable attorneys' fees, and litigation costs, and (iii) empowers district

[100] 18 U.S.C. § 2710(a)(1).

[101] *Id.* § 2710(a)(4).

[102] *Id.* § 2710(a)(3).

[103] *Id.* § 2710(b)(1).

courts to provide appropriate equitable relief.[104]

The plaintiffs allege that Viacom disclosed to Google URL information that effectively revealed what videos they watched on Nickelodeon's websites, and static digital identifiers (such as IP addresses, browser fingerprints, and unique device identifiers) that enabled Google to link the watching of those videos to their real-world identities.[105]

[104] *Id.* § 2710(c)(2)(A)–(D).

[105] Second Compl. ¶¶ 75–76, 143–46. As a technical matter, IP addresses themselves "may be either 'static' (remain constant) or 'dynamic' (change periodically)." *Klimas v. Comcast Cable Commc'ns, Inc.*, 465 F.3d 271, 273 (6th Cir. 2006). Quite apart from this distinction, we use the phrase "static digital identifiers" to refer to the various types of information allegedly disclosed by the defendants, including IP addresses, browser fingerprints, unique device ID numbers, and cookie identifiers. By using the word "static," we mean to convey that these identifiers persisted across time in a manner that allegedly enabled the defendants to identify the plaintiffs and to catalogue their online browsing habits.

They bring claims under the Act against both defendants.[106]

1. Whether Google is an Appropriate Defendant under the Act

The first question we confront is whom, exactly, the Act permits the plaintiffs to sue. The plaintiffs contend that the Act allows them to sue *both* a video tape service provider who discloses personally identifiable information *and* a person who receives that information. To put it another way, the parties seem to agree that the video clerk who leaked Judge Bork's rental history clearly would have been liable under the Act had it been in force at the time—but what about the reporter at the *Washington City Paper* to whom he leaked the information? The plaintiffs say he would have been liable as well. Google (standing-in for the reporter in our fact pattern) disagrees.

The text of the statute is not clear on this point. Subsection (b) states that a "video tape service provider who knowingly discloses, to any person, personally identifiable

[106] The defendants do not argue that the plaintiffs were not "consumers" of Viacom's video services—*i.e.*, persons who "rent[], purchase[], or subscribe[]" to goods or services of a service provider. 18 U.S.C. § 2710(a)(1). We note that the Eleventh Circuit has held that persons who download a free application to watch videos on their smartphones are not "subscribers" under the Act. *See Ellis v. Cartoon Network, Inc.*, 803 F.3d 1251, 1257 (11th Cir. 2015). In the absence of any argument to the contrary, we will assume that the plaintiffs were consumers of Viacom's video services.

information concerning any consumer of such provider shall be liable to the aggrieved person for the relief provided in subsection (c).”[107] Subsection (c), in turn, creates a private cause of action. It states that “[a]ny person aggrieved by any act of a person in violation of this section may bring a civil action in a United States district court.”[108]

But what constitutes a “violation of this section”? Google claims that the Act is violated only when a video tape service provider discloses personally identifiable information, as proscribed in subsection (b). The plaintiffs, by contrast, insist that they are just as “aggrieved” when a third party receives personally identifiable information as when a video tape service provider discloses it. In support of this argument, the plaintiffs rely exclusively on a somewhat dated case from a district court in our Circuit, *Dirkes v. Borough of Runnemede*.[109] We find the plaintiffs’ reliance on *Dirkes* unpersuasive.

---

[107] 18 U.S.C. § 2710(b)(1). Actually, this provision of the Act refers to “the relief provided in subsection (d),” but that is clearly a scrivener’s error. As Judge Posner explained in *Sterk*, “the only ‘relief’ provided [in subsection (d)] is exclusion of the personally identifiable information from evidence,” and “it is very unlikely that a video tape service provider would ever be submitting, as evidence in a legal proceeding, personally identifiable information that the provider had disclosed.” 672 F.3d at 537.

[108] 18 U.S.C. § 2710(c)(1).

[109] 936 F. Supp. 235 (D.N.J. 1996).

Dirkes was a former police officer who was suspected of stealing pornographic videos from a citizen's apartment. The allegations led local prosecutors to indict Dirkes for committing misconduct and led the local police department to open disciplinary proceedings. Even though Dirkes was eventually acquitted of the misconduct charge, the Borough's inquiry continued. A Borough investigator learned from a video store clerk that Dirkes had rented several pornographic movies, and information about Dirkes' video rental history was included in an internal affairs memorandum. That memorandum "was distributed to the Borough's special counsel, who in turn distributed it in connection with Plaintiff Dirkes' disciplinary hearing and in a proceeding before the Superior Court of New Jersey, Camden County."[110]

In response to the dissemination of information about his video rental history, Dirkes and his wife sued the investigator, the police department, and the Borough for violating the Video Privacy Protection Act.[111] The district court rejected the defendants' argument that, as non-disclosing parties, they could not be liable under the Act. Instead, it reasoned that Congress's broad remedial purposes in passing the statute would best be served by allowing

---

[110] *Id.* at 236.

[111] *Id.* Another section of the Act, 18 U.S.C. § 2710(b)(2)(C), permits a video tape service provider to disclose information "to a law enforcement agency pursuant to a warrant . . . , a grand jury subpoena, or a court order." The video clerk in *Dirkes* simply provided the information to the investigating officer when asked. *See Dirkes*, 936 F. Supp. at 236.

plaintiffs to sue "those individuals who have come to possess (and who could disseminate) the private information."[112]

No other court has interpreted the Act this way. As the Sixth Circuit explained in *Daniel v. Cantrell*,[113] the better view is that subsection (b) makes certain conduct—the disclosure of personally identifiable information by a video tape service provider—unlawful, and subsection (c) creates a cause of action against persons who engage in such conduct.[114] Indeed, "if *any* person could be liable under the Act, there would be no need for the Act to define a [video tape service provider] in the first place."[115] Rejecting *Dirkes*' focus on the Act's remedial purposes, *Cantrell* observed that "[j]ust because Congress' goal was to prevent the disclosure of private information, does not mean that Congress intended the implementation of every conceivable method of

---

[112] *Id.* at 240. Alternatively, the district court concluded that the defendants had potentially violated subsection (d) of the Act, which bars the introduction of illegally disclosed information in "any trial, hearing . . . or other proceeding in or before any court . . . department . . . or other authority of the United States, a State, or a political subdivision of a State." *Id.* at 240 n.8. The present case does not require us to opine on the correctness of this interpretation.

[113] 375 F.3d 377 (6th Cir. 2004).

[114] *Id.* at 382–84 (stating that *Dirkes* concluded that any person could be liable for unlawful disclosures "only by misreading the Act").

[115] *Id.* (emphasis in original).

preventing disclosures."[116] The Seventh Circuit adopted the same reading of the Act in *Sterk v. Redbox Automated Retail, LLC*,[117] concluding that "the more plausible interpretation is that [subsection (c)] is limited to enforcing the prohibition of disclosure."[118]

We agree with our colleagues in the Sixth and Seventh Circuits. Because we conclude that only video tape service providers that disclose personally identifiable information can be liable under subsection (c) of the Act, and because Google is not alleged to have disclosed any such information here, we will affirm the District Court's dismissal of the claim against Google.[119]

2. Whether Viacom Disclosed "Personally Identifiable Information"

Viacom also argues that it never disclosed "personally identifiable information" about children who viewed videos on its websites. As we shall see, what counts as personally

---

[116] *Id.* at 384.

[117] 672 F.3d 535.

[118] *Id.* at 538.

[119] The plaintiffs argued before the District Court that Google was a video tape service provider, but did not raise the same argument on appeal. We therefore need not address that argument here. *See United States v. Hoffecker*, 530 F.3d 137, 162 (3d Cir. 2008) (describing "the requirement that an appellant [must] raise an issue in his opening brief or else waive the issue on appeal").

identifiable information under the Act is not entirely clear.

The plaintiffs claim that Viacom disclosed to Google at least eleven pieces of information about children who browsed its websites.[120] Three, in particular, are central to their claim under the Act. The first is a user's IP address, "a number assigned to each device that is connected to the Internet" that permits computer-specific online tracking.[121] The second is a user's browser and operating system settings, which comprise a so-called "browser fingerprint."[122] The plaintiffs claim that these profiles are so detailed that the odds of two people having the same browser fingerprint are 1 in 286,777.[123] The third is a computing device's "unique device identifier."[124]

---

[120] Second Compl. ¶ 143.

[121] *See United States v. Vosburgh*, 602 F.3d 512, 517 n.3 (3d Cir. 2010) ("Although most devices do not have their own, permanent ('static') addresses, in general an IP address for a device connected to the Internet is unique in the sense that no two devices have the same IP address at the same time."). *Vosburgh* affirmed a defendant's conviction for possession of child pornography after FBI agents recorded the defendant's IP address and then subpoenaed the defendant's Internet service provider to learn his identity.

[122] Second Compl. ¶ 61.

[123] *Id.* ¶ 62.

[124] Nowhere in their complaints or in their briefing do the plaintiffs explain what a "unique device identifier" actually is, although other cases give us some indication. For example,

What these pieces of information have in common is that they allegedly permit Google to track the same computer across time. So, for example, if someone with a Google account were to run a Google search from his or her computer, and then that person's child were to visit Nick.com and watch a video on that same computer, the plaintiffs claim that Google could "match" the data (based on IP address, browser fingerprint, or unique device identifier) to determine that the same computer was involved in both activities. In the plaintiffs' view, this means that Viacom, by permitting Google to use cookies on its website, effectively disclosed "information which identifies [a particular child] as having requested or obtained specific video materials or services from a video tape service provider,"[125] thereby violating the Act. The plaintiffs also claim that Viacom acted "knowingly," as the Act requires, because Viacom permitted Google to host ads on its websites despite being "aware of Google's ubiquitous presence on the Internet and its tracking of users."[126]

---

one of the types of information at issue in *Ellis v. Cartoon Network, Inc.*, another case brought under the Video Privacy Protection Act, was the device ID on Android phones. The *Ellis* Court described that ID as "a 64–bit number (hex string) that is randomly generated when a user initially sets up his device and should remain constant for the lifetime of the user's device." 803 F.3d at 1254. Presumably the plaintiffs are referring to something similar.

[125] 18 U.S.C. § 2710(a)(3).

[126] Second Compl. ¶ 93.

Viacom, by contrast, argues that static digital identifiers, such as IP addresses, do not qualify as personally identifiable information. It encourages us to interpret the Act against the backdrop of the problem it was meant to rectify—the disclosure of an actual person's video rental history. So, for example, Viacom points to the Senate Report, which states that "personally identifiable information is intended to be transaction-oriented," meaning that it "identifies a particular person as having engaged in a specific transaction with a video tape service provider."[127] Viacom reads this passage to suggest that the Act's authors had brick-and-mortar transactions in mind when they crafted the law. In Viacom's view, the information described by the plaintiffs is not personally identifiable because it does not, by itself, identify a particular person. Rather, it is "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"—not to unmask the identity of a person using that computer.[128]

The parties' contrasting positions reflect a fundamental disagreement over what kinds of information are sufficiently "personally identifying" for their disclosure to trigger liability under the Video Privacy Protection Act. At one end of the spectrum, of course, is a person's actual name. Then there are pieces of information, such as a telephone number or a physical address, which may not by themselves identify a particular person but from which it would likely be possible to identify a person by consulting publicly available sources,

[127] Senate Report at 12.

[128] Viacom Br. at 16.

such as a phone book or property records. Further down the spectrum are pieces of information, like social security numbers, which are associated with individual persons but might not be easily matched to such persons without consulting another entity, such as a credit reporting agency or government bureau.

The kind of information at issue here—static digital identifiers—falls even further down the spectrum. To an average person, an IP address or a digital code in a cookie file would likely be of little help in trying to identify an actual person. A great deal of copyright litigation, for example, involves illegal downloads of movies or music online. Such suits often begin with a complaint against a "John Doe" defendant based on an Internet user's IP address. Only later, after the plaintiff has connected the IP address to an actual person by means of a subpoena directed to an Internet service provider, is the complaint amended to reflect the defendant's name.[129]

Numerous district courts have grappled with the question of whether the Video Privacy Protection Act applies to static digital identifiers. Most have followed the rule adopted in *In re Hulu Privacy Litigation*.[130] The court there

---

[129] *See, e.g.*, *Warner Bros. Records Inc. v. Walker*, 704 F. Supp. 2d 460, 463 (W.D. Pa. 2010) ("Plaintiffs initially filed this action as a 'Doe' lawsuit and subsequently amended the Complaint after Defendant's identity was obtained from Allegheny College pursuant to a Rule 45 subpoena.").

[130] No. 11-cv-3764 (LB), 2014 WL 1724344 (N.D. Cal. Apr. 28, 2014).

concluded that static digital identifiers that could, in theory, be combined with other information to identify a person do not count as "personally identifiable information" under the Act, at least by themselves.[131] Other decisions are in accord.[132]

The district courts have not, however, been unanimous. The plaintiffs direct us to *Yershov v. Gannett Satellite Information Network, Inc.*[133] The plaintiff there downloaded *USA Today*'s free application onto his smartphone. He alleged that Gannett, which publishes *USA Today*, shared information about videos he watched on his phone with a third-party analytics company, Adobe Systems, Inc. The information did not include the plaintiff's name or address, but rather his cell phone identification number and his GPS coordinates at the time he viewed a particular video.[134] Rejecting the approach taken in *Hulu*, *Yershov* concluded that

---

[131] *Id.* at *11 (concluding that "a unique anonymized ID alone is not [personally identifiable information] but context could render it not anonymous and the equivalent of the identification of a specific person").

[132] *See, e.g.*, *Robinson v. Disney Online*, --- F. Supp. 3d ---, 2015 WL 6161284, at *6 (S.D.N.Y. 2015); *Eichenberger v. ESPN, Inc.*, No. 14-cv-463 (TSZ), 2015 WL 7252985, at *4–5 (W.D. Wash. May 7, 2015); *Ellis v. Cartoon Network, Inc.*, No. 14-cv-484 (TWT), 2014 WL 5023535, at *3 (N.D. Ga. Oct. 8, 2014), *aff'd on other grounds*, 803 F.3d 1251 (11th Cir. 2015).

[133] 104 F. Supp. 3d 135 (D. Mass. 2015).

[134] *Id.* at 138.

any unique identifier—including a person's smartphone ID—is personally identifiable information. It recognized that, in asking it to reach this conclusion, the plaintiff was "attempt[ing] to place a square peg (modern electronic technology) into a round hole (a statute written in 1988 aimed principally at videotape rental services)."[135] Even so, the court stated that the Act applied to the disclosure of static identifiers that could theoretically permit a company like Adobe Systems to identify an individual video watcher.[136] The First Circuit recently affirmed that conclusion.[137]

In our view, the proper meaning of the phrase "personally identifiable information" is not straightforward. As a textual matter, "[t]he precise scope" of such information "is difficult to discern from the face of the statute—whether

---

[135] *Id.* at 140.

[136] *Id.* at 145–46 (discussing *Nickelodeon I* and stating that its "conclusion that '[personally identifiable information] is information which must, without more, itself link an actual person to actual video materials' is flawed").

[137] *Yershov v. Gannett Satellite Info. Network, Inc.*, --- F.3d ---, 2016 WL 1719825, at *2–3 (1st Cir. 2016). Despite its expansive interpretation of what qualifies as personally identifiable information, the district court in *Yershov* concluded that the plaintiff in that case was not a "subscriber" within the meaning of the Video Privacy Protection Act and therefore dismissed the case. The First Circuit reached the opposite conclusion and remanded the case for further proceedings. *See id.* at *3–6.

read in isolation or in its broader statutory context."[138] As a practical matter, norms about what ought to be treated as private information on the Internet are both constantly in flux and often depend on the novelty of the technology at issue. Even so, we find Viacom's narrower understanding of what constitutes "personally identifiable information" under the Act more persuasive than the alternative offered by the plaintiffs.

We begin with principles of statutory interpretation. We have said that when "the text [of a statute] is ambiguous or does not reveal congressional intent 'with sufficient precision' to resolve our inquiry[,] . . . 'a court traditionally refers to the legislative history and the atmosphere in which the statute was enacted in an attempt to determine the congressional purpose.'"[139] Likewise, the Supreme Court had instructed us that "[w]hen technological change has rendered its literal terms ambiguous, [a law] must be construed in light of [its] basic purpose."[140] Our review of the legislative history convinces us that Congress's purpose in passing the Video Privacy Protection Act was quite narrow: to prevent disclosures of information that would, with little or no extra

---

[138] *Disney*, 2015 WL 6161284, at *2.

[139] *Jensen v. Pressler & Pressler*, 791 F.3d 413, 418 (3d Cir. 2015) (quoting, in succession, *Allen ex rel. Martin v. LaSalle Bank, N.A.*, 629 F.3d 364, 367 (3d Cir. 2011), and *In re Lord Abbett Mut. Funds Fee Litig.*, 553 F.3d 248, 254 (3d Cir. 2009)).

[140] *Twentieth Century Music Corp. v. Aiken*, 422 U.S. 151, 156 (1975) (interpreting the Copyright Act).

effort, permit an ordinary recipient to identify a particular person's video-watching habits. We do not think that, when Congress passed the Act, it intended for the law to cover factual circumstances far removed from those that motivated its passage.

This becomes apparent by tracing the Video Privacy Protection Act's legislative history. The Senate version of the Act was introduced in May of 1988, and the coordinate House bill was introduced about a month later. The two bills were considered in a joint hearing in August of 1988 before the relevant House and Senate subcommittees.[141] The then-extant Senate bill would have punished *both* disclosures relating to video tape service providers *and* disclosures relating to library borrowing records.[142] Senator Patrick Leahy, Chairman of the Senate Subcommittee on Technology and the Law, characterized the purpose of the Senate bill as follows:

> Most of us rent movies at video stores and we check out books from our community libraries. These activities generate an enormous report of personal activity that, if it is going to be disclosed, makes it very, very difficult for a

---

[141] Senate Report at 5; *see also Video and Library Privacy Protection Act of 1988: Hearing on H.R. 4947 & S. 2361 Before the Subcomm. on Courts, Civil Liberties & the Admin. of Justice of the H. Comm. on the Judiciary & the Subcomm. on Tech. & the Law of the S. Comm. on the Judiciary*, 100th Cong. (1988) ("Committee Report").

[142] Committee Report at 13–15 (quoting relevant text of S. 2361).

person to protect his or her privacy.

> It really isn't anybody's business what books or what videos somebody gets. It doesn't make any difference if somebody is up for confirmation as a Supreme Court Justice or they are running the local grocery store. It is not your business.[143]

Similarly, Representative Robert Kastenmeier, Chairman of the House Subcommittee on Courts, Civil Liberties, and the Administration of Justice, decried "attempts to obtain patrons' [library] records, under circumstances that . . . would violate most peoples' perceptions of their right to privacy."[144] He expressed the view that "American citizens should not have to worry that a government agent, or a reporter, or anyone else, will be able to find out what they are reading," and argued that "[t]hese principles apply as much to customers of video stores as to patrons of libraries."[145]

According to the Senate Report, the provisions of the Act relating to libraries were removed because the Senate Judiciary Committee "was unable to resolve questions regarding the application of such a provision for law enforcement."[146] Even so, we think that legislators' initial focus on both libraries and video stores indicates that the Act

---

[143] *Id.* at 18.

[144] *Id.* at 21–22.

[145] *Id.* at 22–23.

[146] Senate Report at 8.

was meant to prevent disclosures of information capable of identifying an *actual person's* reading or video-watching habits. We therefore agree with our colleagues who have reviewed this same legislative history and concluded that the Act "protects personally identifiable information that identifies a specific person and ties that person to particular videos that the person watched."[147]

The plaintiffs contend that, contrary to our interpretation, Congress intended to pass a broad statute that would protect consumer privacy even as video-watching technology changed over time. To be fair, there are portions of the legislative history that might be read to support such a view.[148] The text itself is also amenable to such an interpretation. After all, the Act says that personally identifiable information "*includes* information which identifies a person as having requested or obtained specific video materials or services from a video tape service

---

[147] *Hulu*, 2014 WL 1724344, at *8; *see also Eichenberger*, 2015 WL 7252985, at *4 ("The focus of this statute . . . is on whether the disclosure by itself identifies a particular person as having viewed a specific video.").

[148] *See, e.g.*, Committee Report at 19 ("These bills are an effort to keep up to date with changing technology and changing social patterns with respect to the use of materials which ought to be clearly private.") (statement of Representative Kastenmeier); *id.* at 55 ("These precious [privacy] rights have grown increasingly vulnerable with the growth of advanced information technology.") (testimony of Janlori Goldman, Staff Attorney, American Civil Liberties Union).

provider,"[149] and Congress's use of the word "includes" could suggest that Congress intended for future courts to read contemporary norms about privacy into the statute's original text.[150] But we ultimately do not think that the definition of personally identifiable information in the Act is so broad as to cover the kinds of static digital identifiers at issue here. This is not to say that the Act has become a dead letter with the demise of the corner video store. If, for example, Google were to start purposefully leaking its customers' YouTube video-watching histories, we think such disclosures would almost certainly violate the Act. But trying to analogize between that kind of disclosure and Google's use of cookies on Viacom's websites is, at best, a strained enterprise.

Nor are we persuaded by the plaintiffs' citations to other federal privacy laws. For example, the plaintiffs ask us to consider how Congress used the phrase "personally identifiable information" (or its equivalents) in (i) the Children's Online Privacy Protection Act,[151] (ii) the Gramm-Leach Financial Modernization Act,[152] (iii) the Federal

---

[149] 18 U.S.C. § 2710(a)(3) (emphasis added).

[150] *See Yershov*, 2016 WL 1719825, at *2 (noting that "the word 'includes' . . . normally implies that the proffered definition falls short of capturing the whole meaning"); Senate Report at 12 (stating that the use of the word "includes" is intended to "establish a minimum, but not exclusive, definition of personally identifiable information").

[151] 15 U.S.C. § 6501(8).

[152] 15 U.S.C. § 6809(4).

Education Rights and Privacy Act,[153] and (iv) the Health Insurance Portability and Accountability Act.[154] Having done so, we do not think that the language in these other laws is as helpful as the plaintiffs suppose. If anything, the expansion of privacy laws since the Video Privacy Protection Act's passage demonstrates that, whatever else "personally identifiable information" meant in 1988, it did not encompass the kind of information that Viacom allegedly disclosed to Google.

We see this perhaps most clearly by juxtaposing the 1988 Video Privacy Protection Act with the Children's Online Privacy Protection Act ("COPPA"), which Congress passed a decade later.[155] That statute limits the gathering of personal information from children under the age of 13 on the Internet.[156] It also requires parental consent for the collection, use, or disclosure of children's personal information online and directs the Federal Trade Commission to issue regulations

---

[153] 20 U.S.C. § 1232g; *see also* 34 C.F.R. § 99.3 (defining "personally identifiable information" in the education context).

[154] 42 U.S.C. § 1320d(6).

[155] Pub. L. No. 105-277, Div. C, Title XIII, §§ 1301–1308, 112 Stat. 2681–728, *codified at* 15 U.S.C. §§ 6501–6506.

[156] 15 U.S.C. § 6501(1) (defining the term "child" to mean "an individual under the age of 13"), 6501(10)(A)(i)–(ii) (stating that a website "directed to children" is "a commercial website or online service that is targeted to children" or "that portion of a commercial website or online service that is targeted to children").

to that effect.[157] The statute defines "personal information" to include:

> [A] first and last name; a home or other physical address . . . ; an e-mail address; a telephone number; a Social Security number; any other identifier that the [Federal Trade Commission] determines permits the physical or online contacting of a specific individual; or information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph.[158]

The Federal Trade Commission has promulgated two successive rules under this provision. The first, which became effective in April of 2000,[159] defined "personal information" to include not only the kinds of information enumerated in the text of the law, but also "[a] persistent identifier, such as a customer number held in a cookie or a

---

[157] *Id.* § 6502(a)(1) (requiring compliance with regulations), 6502(b)(1) (delegating authority to the Commission), 6502(b)(1)(A)(ii) (directing the Commission to establish regulations requiring the "verifiable parental consent for the collection, use, or disclosure of personal information from children").

[158] *Id.* § 6501(8)(A)–(G).

[159] *See* Children's Online Privacy Protection Rule, 64 Fed. Reg. 59,888 (Nov. 3, 1999), *available at* 1999 WL 990699 (promulgating final rule to be codified at 16 C.F.R. § 312).

processor serial number, where such identifier is associated with individually identifiable information."[160] An updated regulation, effective in July of 2013,[161] expanded this definition to include any "persistent identifier that can be used to recognize a user *over time and across different Web sites or online services*," including but not limited to "a customer number held in a cookie, an Internet Protocol (IP) address, a processor or device serial number, or unique device identifier."[162]

It seems clear that the Commission's updated definition of "personal information" comes much closer to capturing, if not wholly covering, the kinds of information at issue in this case.[163] But that is of little help to the plaintiffs' present claim. Instead, the evolution of these regulations demonstrates that, when Congress passed COPPA, it gave the Federal Trade Commission authority to *expand* the types of

---

[160] 16 C.F.R. § 312.2 (2000).

[161] Children's Online Privacy Protection Rule, 78 Fed. Reg. 3,972 (Jan. 17, 2013), *available at* 2013 WL 169584 (promulgating updated rule).

[162] 16 C.F.R. § 312.2 (2013) (emphasis added).

[163] The Federal Trade Commission's first definition of "personal information" would seemingly *not* cover the kind of information at issue here because, while that definition did include a reference to numerical codes stored in cookies, it also required such codes to be linked to the other kinds of information listed in the statute. Gender and birthdate, the two kinds of information Viacom allegedly collected when children signed up for its websites, are not on that list.

information that count as personally identifying under that law. In this way, Congress built flexibility into the statute to keep pace with evolving technology. The Video Privacy Protection Act, by contrast, does not empower an administrative agency to augment the definition of "personally identifiable information" in light of changing circumstances or new technologies. The meaning of that phrase in the Act is, it would appear, more static.

Subsequent developments confirm this view. Congress amended the Video Privacy Protection in 2013,[164] modifying those provisions of the law governing how a consumer can consent to the disclosure of personally identifiable information.[165] The legislative history of the 2013 amendments demonstrates that Congress was keenly aware of how technological changes have affected the original Act. As one Senate report put it:

> At the time of the [1988 law's] enactment, consumers rented movies from video stores. The method that Americans used to watch videos in 1988—the VHS cassette tape—is now

[164] Pub. L. No. 112-258, 126 Stat. 2414. While Congress did not pass the law until January of 2013, it is titled the "Video Privacy Protection Act Amendments Act of 2012."

[165] *See Ellis*, 803 F.3d at 1253 (explaining that these "changes allowed consumers greater flexibility to share their video viewing preferences, while maintaining their privacy, by clarifying that video tape service providers may obtain informed, written consent of consumers on an ongoing basis via the Internet").

> obsolete. In its place, the Internet has revolutionized the way that American consumers rent and watch movies and television programs. Today, so-called "on-demand" cable services and Internet streaming services allow consumers to watch movies or TV shows on televisions, laptop computers, and cell phones.[166]

Despite this recognition, Congress did not update the definition of personally identifiable information in the statute.[167] What's more, it chose not to do so despite the fact that the *amicus* supporting the plaintiffs here, the Electronic Privacy Information Center, submitted written testimony that included the following exhortation:

> [T]he Act does not explicitly include Internet Protocol (IP) Addresses in the definition [of personally identifiable information]. IP addresses can be used to identify users and link consumers to digital video rentals. They are akin to Internet versions of consumers' home telephone numbers. . . . We would propose the addition of Internet Protocol (IP) Addresses and account identifiers to the

[166] S. Rep. No. 112-258, at 2 (2012).

[167] *See* H.R. Rep. No. 112-312, at 3 (2011) (noting that the updated version of the legislation "does not change . . . the definition of 'personally identifiable information'").

> definition of [personally identifiable information] . . . .[168]

We think Congress's decision to retain the 1988 definition of personally identifiable information indicates that the Act serves different purposes, and protects different constituencies, than other, broader privacy laws. We of course appreciate that the passage of time often requires courts to apply old laws in new circumstances.[169] Assessing congressional intent in these cases can be difficult; indeed, Congress may not have considered the temporal problem at all. But here, our task is made easier by the fact that Congress has recently revisited the Video Privacy Protection Act and, despite the passage of nearly thirty years since its enactment, left the law almost entirely unchanged. We have previously explained that "the weight given subsequent legislation and whether it constitutes a clarification or a repeal is a context-

---

[168] *The Video Privacy Protection Act: Protecting Viewer Privacy in the 21st Century: Hearing Before the Subcomm. on Privacy, Tech. and the Law of the S. Comm. on the Judiciary*, 112th Cong. 59–60 (2012).

[169] *See, e.g., Del. Dep't of Nat. Res. & Envtl. Control v. U.S. Army Corps of Eng'rs*, 685 F.3d 259, 284 (3d Cir. 2012) (stating that it would arguably "be irrational" to interpret a statutory directive to "maintain navigation," inserted into a law in 1977, "to encompass only those activities that preserve bodies of water as they existed in 1977"); *United States v. Dire*, 680 F.3d 446, 467 (4th Cir. 2012) (concluding that Congress defined piracy in 1819 to reflect the evolving "law of nations" and rejecting the proposition "that the definition of general piracy was fixed in the early Nineteenth Century").

and fact-dependent inquiry,"[170] and "we may pay heed to the significance of subsequent legislation when it is apparent from the facts and context that it bears directly on Congress's own understanding and intent."[171] We think Congress's decision to leave the Act's 1988 definition of personally identifiable information intact, despite recently revisiting the law, is one of those instances.

Nor does our decision today create a split with our colleagues in the First Circuit. In interpreting the meaning of personally identifiable information in *Yershov*, the First Circuit focused on the fact that the defendant there allegedly disclosed not only what videos a person watched on his or her smartphone, but also the GPS coordinates of the phone's location at the time the videos were watched. In the First Circuit's view, "[g]iven how easy it is to locate a GPS coordinate on a street map, this disclosure would enable most people to identify what are likely the home and work addresses of the viewer (*e.g.*, Judge Bork's home and the federal courthouse)."[172] That conclusion merely demonstrates that GPS coordinates contain more power to identify a *specific person* than, in our view, an IP address, a device identifier, or a browser fingerprint. *Yershov* itself acknowledges that "there is certainly a point at which the

---

[170] *Bd. of Trs. of IBT Local 863 Pension Fund v. C & S Wholesale Grocers, Inc.*, 802 F.3d 534, 546 (3d Cir. 2015).

[171] *Sikkelee v. Precision Airmotive Corp.*, --- F.3d ---, 2016 WL 1567236, at *14 (3d Cir. 2016).

[172] *Yershov*, 2016 WL 1719825, at *3 (internal footnote omitted).

linkage of information to identity becomes too uncertain, or too dependent on too much yet-to-be-done, or unforeseeable detective work" to trigger liability under this statute.[173] We believe the information allegedly disclosed here is on that side of the divide.[174]

Of course, what we have said so far addresses the question of what counts as personally identifiable information in the abstract. The wrinkle in this case is that the party to

---

[173] *Id.*

[174] We note, however, that even a numeric identifier might qualify as personally identifiable information, at least in certain circumstances. In *Hulu*, for example, the plaintiffs alleged that when someone visited Hulu's website and watched a video, Hulu would display a Facebook "Like" button next to that video by sending a coded request to Facebook's servers. Before sending that request, Hulu would check to see if the user *already* had cookies on his or her machine indicating that the user was a Facebook member. If so, Hulu would transmit that coded information to Facebook when it requested a "Like" button in such a way that Facebook could easily identify an account holder's video preferences. *See Hulu*, 2014 WL 1724344, at *5.

Hulu concluded that such communications were "not merely the transmission of a unique, anonymous ID," but rather the disclosure of "information that identifies the Hulu user's actual identity on Facebook," which, in the court's view, was sufficient to count as personally identifiable information. *Id.* at *13. Whether we would reach a similar conclusion on analogous facts we leave to a later case.

whom the plaintiffs' information was disclosed is Google, a company whose entire business model is purportedly driven by the aggregation of information about Internet users. The plaintiffs assert that Google can identify web users in the real world, and indeed seem to believe that Google, which purportedly "knows more details about American consumers than any company in history,"[175] aggregates so much information that it has, in effect, turned the Internet into its own private data collection machine. Or, as the plaintiffs' *amicus*, the Electronic Privacy Information Center, puts it, concluding "that Google is unable to identify a user based on a combination of IP address . . . and other browser cookie data . . . would be like concluding the company that produces the phone book is unable to deduce the identity of an individual based on their telephone number."[176]

Whether or not this is true, we do not think that a law from 1988 can be fairly read to incorporate such a contemporary understanding of Internet privacy. The allegation that Google will assemble otherwise anonymous pieces of data to unmask the identity of individual children is, at least with respect to the kind of identifiers at issue here, simply too hypothetical to support liability under the Video Privacy Protection Act.

The argument also lacks a limiting principle. What makes the claim about Google's ubiquity so intuitively attractive is the size of Google's user base. Indeed, Google is large enough that we might well suppose that a significant

---

[175] Pls. Br. at 10.

[176] Electronic Privacy Information Center Br. at 6.

number of its account holders also have children who watch videos on Viacom's websites. But that seems like distinction without a difference. If an IP address were to count as personally identifiable information, either standing alone or coupled with similar data points, then the disclosure of an IP address to *any* Internet company with registered users might trigger liability under the Act. Indeed, the import of the plaintiffs' position seems to be that the use of third-party cookies on any website that streams video content is presumptively illegal. We do not think the Video Privacy Protection Act sweeps quite so broadly.

We recognize that our interpretation of the phrase "personally identifiable information" has not resulted in a single-sentence holding capable of mechanistically deciding future cases. We have not endeavored to craft such a rule, nor do we think, given the rapid pace of technological change in our digital era, such a rule would even be advisable.[177] Rather, we have tried to articulate a more general framework. In our view, personally identifiable information under the Video Privacy Protection Act means the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior. The classic example will always be a video clerk leaking an individual customer's video rental history. Every step away from that

[177] Pursuant to the First Circuit's reasoning in *Yershov*, if technology were to develop permitting an ordinary person to type an IP address into a search engine and reveal the identity of the person whose computer was associated with that IP address, the same facts alleged here might well result in a different outcome than the one we reach today.

1988 paradigm will make it harder for a plaintiff to make out a successful claim. Some disclosures predicated on new technology, such as the dissemination of precise GPS coordinates or customer ID numbers, may suffice. But others—including the kinds of disclosures described by the plaintiffs here—are simply too far afield from the circumstances that motivated the Act's passage to trigger liability.

Our decision necessarily leaves some unanswered questions about what kinds of disclosures violate the Video Privacy Protection Act. Such uncertainty is ultimately a consequence of our common-law system of adjudication and the rapid evolution of contemporary technology. In the meantime, companies in the business of streaming digital video are well advised to think carefully about customer notice and consent. Whether other kinds of disclosure will trigger liability under the Act is another question for another day.

B. Intrusion upon Seclusion

Lastly, we turn to the plaintiffs' claim that Viacom and Google unlawfully invaded their privacy. In New Jersey, invasion of privacy is an umbrella category that includes a

number of distinct torts.[178] The plaintiffs assert that the defendants committed the tort of intrusion upon seclusion, a type of invasion of privacy involving encroachment on a person's reasonable expectations of solitude. They rest this claim on the allegation that the Nickelodeon website included a message that read: "HEY GROWN-UPS: We don't collect ANY personal information about your kids. Which means we couldn't share it even if we wanted to!"[179] This message appeared on the webpage that children used to register for website accounts, apparently to calm parental fears over the tracking of their children's online activities. In light of this message, the plaintiffs assert that Viacom collected personal information about children, and permitted Google to do the same, despite its assurances that it would not collect "ANY personal information" at all.

1. The Plaintiffs' Intrusion Claim Is Not Preempted

We begin with a threshold issue. Viacom argues that the plaintiffs' intrusion claim is preempted by COPPA, which bars state governments from "impos[ing] any liability for commercial activities" in a way that is "inconsistent with

---

[178] *See Rumbauskas v. Cantor*, 649 A.2d 853, 856 (N.J. 1994) (explaining that invasion of privacy "is not one tort, but a complex of four . . . tied together by the common name, but otherwise hav[ing] almost nothing in common except that each represents an interference with the right of the plaintiff 'to be let alone'" (quoting William L. Prosser, The Law of Torts § 112 (3d ed. 1964)).

[179] Second Compl. ¶ 103.

[COPPA's] treatment of those activities."[180] As we discussed previously, COPPA directs the Federal Trade Commission to issue rules regarding the "collection, use, or disclosure of personal information from children" online, including rules governing parental notice and consent.[181] Since the Commission only recently updated its definition of "personal information" to include the kinds of static digital identifiers (such as IP addresses) that underlie the plaintiffs' allegations, Viacom asserts that the plaintiffs' intrusion claim is "inconsistent" with the treatment of such information under COPPA.[182]

In making this argument, Viacom faces an uphill battle. This is because we apply a general presumption against preemption, meaning that, "[i]n areas of traditional state regulation, we assume that a federal statute has not supplanted state law unless Congress has made such an intention 'clear and manifest.'"[183] This presumption "is relevant even when there is an express pre-emption clause . . . because when the text of a pre-emption clause is susceptible of more than one plausible reading, courts

[180] 15 U.S.C. § 6502(d).

[181] *Id.* § 6502(b)(1)(A).

[182] *See* Viacom Br. at 38 (citing 15 U.S.C. § 6502(d)).

[183] *MD Mall Assocs., LLC v. CSX Transp., Inc.*, 715 F.3d 479, 489 (3d Cir. 2013), *as amended* (May 30, 2013) (quoting *Bates v. Dow Agrosciences, LLC*, 544 U.S. 431, 449 (2005)).

ordinarily accept the reading that disfavors pre-emption."[184] The Supreme Court has also made clear that, even when federal laws have preemptive effect in some contexts, states generally retain their right "to provide a traditional damages remedy for violations of common-law duties when those duties parallel federal requirements."[185]

The question we confront, therefore, is whether the plaintiffs' intrusion claim is truly "inconsistent" with the obligations imposed by COPPA, or whether the plaintiffs' intrusion claim rests on common-law duties that are compatible with those obligations. Because we reach the latter conclusion, Viacom's preemption argument is unavailing.

In our view, the wrong at the heart of the plaintiffs' intrusion claim is not that Viacom and Google *collected* children's personal information, or even that they *disclosed* it. Rather, it is that Viacom created an expectation of privacy on its websites and then obtained the plaintiffs' personal information under false pretenses. Understood this way, there is no conflict between the plaintiffs' intrusion claim and COPPA. While COPPA certainly regulates whether personal information can be collected from children in the first

---

[184] *Id.* (quoting *Franks Inv. Co. LLC v. Union Pac. R.R. Co.*, 593 F.3d 404, 407 (5th Cir. 2010) (additional internal quotation marks omitted)).

[185] *Medtronic, Inc. v. Lohr*, 518 U.S. 470, 495 (1996); *see also Riegel v. Medtronic, Inc.*, 552 U.S. 312, 330 (2008) (continuing to recognize that "parallel" state-law claims may be permissible even in the context of express preemption).

instance, it says nothing about whether such information can be collected using deceitful tactics. Applying the presumption against preemption, we conclude that COPPA leaves the states free to police this kind of deceptive conduct.[186]

Indeed, we confronted a similar allegation last year in *Google*. The plaintiffs there alleged that Google had evaded browser-based cookie blockers even as "it held itself out as respecting" them.[187] We concluded that the alleged gap between Google's public-facing comments and its actual behavior was problematic enough for a jury to conclude that Google committed "an egregious breach of social norms."[188] In our view, the problem was not disclosure *per se*. Rather, "[w]hat [was] notable . . . [was] *how* Google accomplished its tracking"—*i.e.*, through "deceit and disregard . . . [that]

---

[186] One might argue that if the kinds of static digital identifiers at issue here do not count as personally identifiable information under the Video Privacy Protection Act, they cannot count as "personal information" of the sort that Viacom promised not to collect. We disagree. First, the phrase "personally identifiable information" in the Act is a term of art properly understood in its legislative and historical context. Second, the meaning of Viacom's promise to parents—"We don't collect ANY personal information about your kids"—is better left to a reasonable factfinder who can interpret that guarantee just as any other layperson browsing the Nickelodeon website might do so.

[187] *Google*, 806 F.3d. at 151.

[188] *Id.* (quoting the *Google* plaintiffs' complaint)

raise[d] different issues than tracking or disclosure alone."[189] In those circumstances, "a reasonable factfinder could indeed deem Google's conduct highly offensive or an egregious breach of social norms."[190] We think the same is true here.[191]

Accordingly, we conclude that COPPA does not preempt the plaintiffs' state-law claim for intrusion upon seclusion.

2. The Plaintiffs Have Adequately Alleged an Intrusion Claim

The next question is whether the plaintiffs have adequately alleged the elements of an intrusion claim. The

---

[189] *Id.* at 150 (emphasis in original).

[190] *Id.* at 151 (internal quotation marks omitted).

[191] While consideration of what a reasonable jury might conclude is normally appropriate at the summary judgment stage, we think it is also appropriate here given the nature of the common law tort at issue. In *Google*, for example, we considered the plaintiffs' allegations from the perspective of a reasonable factfinder because, under California law, privacy torts involve mixed questions of law and fact. *See id.* at 150 n.119. New Jersey law appears to be similar. *Cf. Castro v. NYT Television*, 895 A.2d 1173, 1177–78 (N.J. Super. Ct. App. Div. 2006) (noting that "a trier of fact could find that the videotaping of some patients at Jersey Shore would not support imposition of liability for invasion of privacy," but could also find that "[the defendant's] videotaping of other patients satisfied all the elements of this cause of action").

New Jersey Supreme Court, looking to the Second Restatement of Torts, has said that intrusion upon seclusion occurs whenever a plaintiff can show (i) an intentional intrusion (ii) upon the seclusion of another that is (iii) highly offensive to a reasonable person.[192] At least with respect to Viacom, we conclude that the plaintiffs have adequately alleged each of these three elements.

First, the plaintiffs have successfully alleged an "intentional intrusion." We considered this issue in *O'Donnell v. United States*,[193] where we stated that "an actor commits an *intentional* intrusion only if he believes, or is substantially certain, that he lacks the necessary legal or personal permission to commit the intrusive act."[194] The defendants contend that *O'Donnell* bars the present claim because, after all, they installed cookies on the plaintiffs'

---

[192] *Hennessey v. Coastal Eagle Point Oil Co.*, 609 A.2d 11, 17 (N.J. 1992) (citing Restatement (Second) of Torts § 652B (1977)).

[193] 891 F.2d 1079 (3d Cir. 1989).

[194] *Id.* at 1083 (emphasis in original). While *O'Donnell* arose under Pennsylvania rather than New Jersey law, we concluded that the Pennsylvania Supreme Court was likely to adopt the definition of intrusion upon seclusion included in the Second Restatement of Torts. *See id.* at 1082 n.1. The Pennsylvania Supreme Court later did so in *Burger v. Blair Medical Associates*, 964 A.2d 374, 379 & n.5 (Pa. 2004). Since the highest courts of both New Jersey and Pennsylvania have looked to the same treatise, we are comfortable adopting our reasoning in *O'Donnell* for present purposes.

computers under the belief that doing so was perfectly legal. While we appreciate the force of this argument, we do not think that the plaintiffs' claim is so easily scuttled.

In the first place, *O'Donnell* is factually distinguishable. That case involved the allegedly unlawful disclosure of medical records by the Veterans Administration. Discovery revealed that "O'Donnell had authorized the [Veterans Administration] on previous occasions to view these records and disclose them."[195] We therefore concluded that there was "no dispute of material fact concerning the . . . lack of any intention to invade the plaintiff's right to seclusion and privacy."[196] The allegations here, by contrast, are devoid of any suggestion that the plaintiffs ever authorized Viacom and Google to collect or disclose their personal information.

Indeed, *O'Donnell* itself focused on whether the alleged intrusion occurred without "legal *or* personal permission."[197] Courts applying *O'Donnell* have appropriately treated the presence or absence of consent as a

[195] *O'Donnell*, 891 F.2d at 1083.

[196] *Id.*

[197] *Id.* (emphasis added).

key factor in making this assessment.[198] Whatever else the plaintiffs allege, they clearly assert that the defendants tracked their online behavior without their permission to do so. We therefore conclude that, accepting their factual allegations as true, the plaintiffs have successfully stated the first element of an intrusion claim.

Second, the plaintiffs have adequately alleged that the defendants invaded their privacy. We have embraced the Second Restatement's view that liability for intrusion only arises "when [the defendant] has intruded into a private place, or has otherwise invaded a private seclusion that the plaintiff has thrown about his person or affairs."[199] We think that a reasonable factfinder could conclude that Viacom's promise not to collect "ANY personal information" from children *itself* created an expectation of privacy with respect to

---

[198] *See, e.g.*, *Gabriel v. Giant Eagle, Inc.*, 124 F. Supp. 3d 550, 572 (W.D. Pa. 2015) (stating there was no intrusion claim where the personal information in question was "voluntarily provided" to the defendant); *Muhammad v. United States*, 884 F. Supp. 2d 306, 317 (E.D. Pa. 2012) (concluding that the plaintiff adequately alleged intrusion by federal agents who, among other actions, entered his home "without consent or a search warrant"); *Jevic v. Coca Cola Bottling Co. of N.Y.*, No. 89-cv-4431 (NHP), 1990 WL 109851, at *9 (D.N.J. June 6, 1990) ("[O]ne cannot intrude when one has permission.").

[199] *Kline v. Sec. Guards, Inc.*, 386 F.3d 246, 260 (3d Cir. 2004) (quoting *Harris v. Easton Publ'g Co.*, 483 A.2d 1377, 1383 (Pa. Super. Ct. 1984) (citing Restatement (Second) of Torts § 652B cmt. c)).

browsing activity on the Nickelodeon website.

Third, the plaintiffs have adequately alleged, at least with respect to Viacom, that the intrusion on their privacy was "highly offensive to the ordinary reasonable man."[200] The defendants disagree, contending that the use of cookies for benign commercial purposes has become so widely accepted a part of Internet commerce that it cannot possibly be considered "highly offensive." They also assert that the intrusion tort is more appropriately reserved for punishing behavior that is so offensive as to inspire out-and-out revulsion, as opposed to policing online business practices.[201] The District Court felt the same way, concluding that the plaintiffs never explained "how Defendants' collection and monetization of online information would be offensive to the reasonable person, let alone exceedingly so."[202]

---

[200] *Stengart v. Loving Care Agency, Inc.*, 990 A.2d 650, 660 (N.J. 2010) (quoting Restatement (Second) of Torts § 652B cmt. d).

[201] *See, e.g.*, *Leang v. Jersey City Bd. of Educ.*, 969 A.2d 1097, 1115–17 (N.J. 2009) (permitting an intrusion upon seclusion claim to proceed where a coworker falsely reported that a teacher was threatening to kill people, leading to hospitalization and physically invasive searches); *Soliman v. Kushner Cos., Inc.*, 77 A.3d 1214, 1225–26 (N.J. Super. Ct. App. Div. 2013) (permitting a claim to proceed where the defendant installed hidden video cameras in bathrooms).

[202] *Nickelodeon I*, 2014 WL 3012873, at *19; *see also Nickelodeon II*, 2015 WL 248334, at *5–6 (adhering to prior opinion).

With respect to Google, we agree with the District Court. As Google fairly points out, courts have long understood that tracking cookies can serve legitimate commercial purposes.[203] The plaintiffs do not challenge the proposition that the use of "cookies on websites geared toward adults" is generally acceptable,[204] instead falling back on the claim that the use of cookies to track *children* is particularly odious. We are not so sure. Google used third-party cookies on Nick.com in the same way that it deploys cookies on myriad others websites. Its decision to do so here does not strike us as sufficiently offensive, standing alone, to survive a motion to dismiss.[205]

As to Viacom, however, our conclusion is different. In the same way that Viacom's message to parents about not collecting children's personal information may have created

---

[203] *See, e.g.*, *In re DoubleClick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 519 (S.D.N.Y. 2001) ("DoubleClick's purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money by providing a valued service to commercial Web sites.").

[204] Pls. Reply Br. at 29.

[205] Accordingly, we agree with the view of our colleagues, previously expressed in a non-precedential opinion, that courts may decide the "'highly offensive' issue as a matter of law at the pleading stage when appropriate." *Boring v. Google, Inc.*, 362 F. App'x 273, 279–80 (3d Cir. 2010) (affirming dismissal of a lawsuit alleging that Google invaded the plaintiffs' privacy when its "Street View" truck took photographs of the road outside their house).

an expectation of privacy on Viacom's websites, it also may have encouraged parents to permit their children to browse those websites under false pretenses. We recognize that some cases suggest that a violation of a technology company's privacy-related terms of service is not offensive enough to make out a claim for invasion of privacy.[206] Even so, our decision in *Google* compels us to reach a different result. Just as *Google* concluded that a company may commit intrusion upon seclusion by collecting information using duplicitous tactics, we think that a reasonable jury could reach a similar conclusion with respect to Viacom.

We will therefore affirm the District Court's dismissal of the intrusion upon seclusion claim with respect to Google. With respect to Viacom, however, we will vacate the District Court's dismissal and remand for further proceedings.

IV. Conclusion

Several of the plaintiffs' claims are no longer viable after *Google*. These include their claims under the Wiretap Act, the Stored Communications Act, and the California Invasion of Privacy Act. The plaintiffs' claim under the New Jersey Computer Related Offenses Act is also unavailing.

The plaintiffs have also failed to state a claim under

---

[206] *See, e.g.*, *Yunker v. Pandora Media, Inc.*, No. 11-cv-3113 (JSW), 2013 WL 1282980, at *15 (N.D. Cal. Mar. 26, 2013) (relying on California precedent to conclude that the disclosure of personal information in purported violation of music streaming company's terms of service was not highly offensive).

the Video Privacy Protection Act. Their claim against Google fails because the Act permits the plaintiffs to sue only entities that disclose protected information, not parties, such as Google, alleged to be mere recipients of it. Their claim against Viacom fails because the definition of personally identifiable information in the Act does not extend to the kind of static digital identifiers allegedly disclosed by Viacom to Google.

Lastly, we will partially vacate the District Court's dismissal of the plaintiffs' claim for intrusion upon seclusion. *Google* teaches that such a claim may be strong enough to survive a motion to dismiss when a company promises to respect consumer privacy and then disregards its commitment. The plaintiffs have adequately alleged that Viacom collected personal information about children despite its promise not to do so, and we further believe that a reasonable jury could conclude that Viacom's conduct in breach of its promise was highly offensive under New Jersey law.

We will therefore affirm the District Court's dismissal of all claims except the plaintiffs' claim against Viacom for intrusion upon seclusion, which we will remand for further proceedings consistent with this Opinion.