

## ***In re Nickelodeon Consumer Privacy Litigation: An IP Address Is Not Always Personally Identifiable Information***

**8/1/2016**

**By Jane E. Brown**

**What's the Case About?** *In re Nickelodeon Consumer Privacy Litigation*<sup>1</sup> is a multi-district consolidated class action filed on behalf of children under the age of thirteen alleging that Viacom used child directed websites it owned to collect, without parental consent, data from the class members which it then provided to co-defendant Google. The data Viacom captured from children included their gender, birthdate, IP address, the webpages visited and the names of videos the children viewed. The court considered an issue of first impression as to whether an IP address is personally identifiable information (PII) under the Video Privacy Protection Act (VPPA) and whether the collection of the data constituted intrusion upon seclusion under New Jersey law. Plaintiffs argued that the vulnerability of children coupled with public aversion to mining them for data supported liability of Viacom.<sup>2</sup>

**VPPA allegations dismissed:** The court held that Viacom did not violate the VPPA by collecting the IP addresses of children. The decision was based in part, on the precedent set by *In re Hulu Privacy Litigation*.<sup>3</sup> The *Hulu* court determined that static digital identifiers such as IP addresses identify the location of a computer, which, without additional information, cannot be used to identify an individual. Under this rationale, an IP address is not PII, because an address alone cannot “reasonably” lead to the identification of a person. The court also noted that the VPPA is just too old and brittle to encompass technology so distant from its origins as a by-product of Blockbuster, Erol’s Video Club and Hollywood Video stores. A nuance as to why Google escaped liability under VPPA for another reason is touched upon below.

**New Jersey state law claims remanded:** The court remanded the claim against Viacom for violation of the New Jersey intrusion upon seclusion law. The court did not look favorably upon Viacom’s failure to honor its notice to parents that it would not collect any data from children.

---

<sup>1</sup> *In re Nickelodeon Consumer Privacy Litigation*, 2016 WL 3513782 No. 15-1441 (3rd Cir. Jun. 28, 2016).

<sup>2</sup> *Id.* at \* 4 (alleging that (1) targeting ads to children is more profitable than targeting ads to adults, in part, “because children are generally unable to distinguish between content and advertisements;” (2) 80% and 90% of 2,000 adult respondents, respectively, oppose an advertiser’s tracking of children and believed advertisers should obtain a parent’s permission before installing cookies on a device used by a minor child; and (3) companies can use “browser fingerprinting” to identify specific users).

<sup>3</sup> *In re Hulu Privacy Litigation*, No. 11-CV-3764 (LB), 2014 WL 1724344 (N.D. Cal. Apr. 28, 2014).

**The allegations against Viacom:** Viacom owns the websites, Nick.Jr. and Nick.com (Nick Sites), both of which are associated with the Nickelodeon channel. The Nick Sites offer games and streaming videos to children and included this notice to 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!”<sup>4</sup>

When children registered on one of the Nick Sites, they received a nickname of an avatar based on a Nickelodeon cartoon character of the same gender and approximate age as the child. The plaintiffs alleged that Viacom used first-party cookies it placed on the children’s computers to obtain information about which games and videos the children accessed. Viacom disclosed the information it collected to Google and permitted Google to place ads on the Nick Sites.

**The allegations against Google:** The plaintiffs alleged that Google (1) placed third-party cookies via advertisement on the computers of children who accessed the Nick Sites, (2) used those cookies to track the children on any website displaying a Google ad, and (3) used “Doubleclick.net cookies”<sup>5</sup> to track the browsing of whomever used the computer across any website Google owned, such as Gmail, YouTube and Google Maps.

**Analysis of the VPPA:** Congress enacted the VPPA after the 1987 Senate Judiciary Committee’s hearings regarding Supreme Court nominee, Robert Bork. During the hearings, a newspaper obtained and publicized a list of titles of 146 films Judge Bork or members of his family rented from a local video store.<sup>6</sup> The list of videos was, even by 1987 standards, unremarkable — not a single NC-17 film on the list. Congress agreed, however, that a person’s video viewing history should be private. Consequently, under the VPPA, a user must give permission for his or her video viewing data to be shared. How does this translate to current technology? It doesn’t. The court likened applying the VPPA to internet technology to putting a square peg in a round hole.<sup>7</sup> Additionally, the court referred to the VPPA as a rigid law that lacked the flexibility of the Children’s Online Privacy Protection Act (COPPA) to regulate effectively technology that is “in flux.”<sup>8</sup>

The key definitions under the VPPA are:

**Consumer:** any renter, purchaser or subscriber of goods or services from a video tape service provider.

**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.

---

<sup>4</sup> *In re Nickelodeon*, 2016 WL 3513782 No. 15-1441 at \* 3 (3rd Cir. Jun. 28, 2016).

<sup>5</sup> *Id.*

<sup>6</sup> Michael Dolan, “The Bork Tapes,” *City Paper*, Sept. 25–Oct. 1, 1987, at 1.

<sup>7</sup> *In re Nickelodeon*, 2016 WL 3513782 No. 15-1441 at \* 15 (3rd Cir. Jun. 28, 2016).

<sup>8</sup> *Id.*, at \* 16-19.

**Personally identifiable information (PII):** includes information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider.

18 U.S.C. § 2710(a). A violation of the VPPA occurs when “[a] video tape service provider ... knowingly disclose[d], to any person, personally identifiable information concerning any consumer of such provider.” *Id.*

**The VPPA was created to protect information specific to viewers of movies.** The court noted that if the definition of PII was expanded for all statutes to include an IP address, there would be no end to litigation and the distinctions between the groups protected by certain statutes would be eroded. Congress’ decision to omit a new definition of PII in the 2013 amendment of the VPPA further emphasized that the VPPA “serves different purposes, and protects different constituencies, than other, broader privacy laws.”<sup>9</sup> For example, if “Google were to start purposefully leaking its customers’ YouTube video-watching histories,” the VPPA “would almost certainly” be violated.<sup>10</sup>

**Extending the VPPA to regulate current technology would likely result in unlimited violations.** Defining an IP address as PII within the context of the VPPA would mean that “the disclosure of an IP address to any Internet company with registered users might trigger “liability” when an IP address is regularly transmitted to an Internet service provider (ISP) with each search.<sup>11</sup> The court also pointed out that there is a spectrum of PII, with first and last name at one end, and an IP address at the other, lower, end of the spectrum, given that the IP address alone may be insufficient to identify a person. The case cited by the court to illustrate the need for a subpoena to identify a person is a copyright infringement case, *Warner Bros. Records Inc. v. Walker*, 704 F.Supp. 2d 460 (W.D. Pa. 2010). Warner Bros. needed a subpoena to identify the student who was assigned the IP address used to illegally download some songs. The student, who shared a room with multiple roommates, possibly would not have been identified without a subpoena, given that several people may have used the computer. It was not “reasonably” likely for Warner Bros. to identify the person responsible for the downloads without a subpoena. Understandably, a subpoena may be necessary in a fluid environment such as a college where multiple people may have access to a computer.

**Time-out:** It’s one thing for Warner Bros. to need help from the college to identify which of multiple people may have used an IP address assigned by the college. It’s something altogether different when Google, which the court describes as “a company whose entire business model is purportedly driven by the aggregation of information about Internet users,” wants to identify a person. The plaintiffs’ *amicus* very astutely provided some real-world perspective about what happens when Google wants to find out who you are: “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.’”<sup>12</sup> Enough said. Resume play.

<sup>9</sup> *In re Nickelodeon*, 2016 WL 3513782 No.: 15-1441 \* 19 (3rd Cir. Jun. 28, 2016).

<sup>10</sup> *Id.* at \* 17.

<sup>11</sup> *Id.* at \* 20-21.

<sup>12</sup> *Id.* at \* 20.

**The court affirmed the dismissal of intrusion upon seclusion claim against Google:** Although the court acknowledged that many people, and some courts, find the monetization and collection of data from children without parental consent repugnant, those acts alone, did not establish a claim for intrusion upon seclusion. Under New Jersey law, an intrusion upon seclusion claim occurs upon a showing that (i) an intentional intrusion (ii) upon the seclusion of another that is (iii) highly offensive to a reasonable person.<sup>13</sup> The court disregarded the fact that children, instead of adults, were tracked, because third-party cookies serve a legitimate commercial purpose for advertisers and Google uses them on the Nick Sites the same way it uses them on other non-child directed sites.

**This is why Viacom may be liable for intrusion upon seclusion:** When Viacom notified parents that it did not collect any personal information about children, it was reasonable for a jury to decide that parents may have permitted their children unsupervised access to the Nick Sites based on the disclaimer. If the parents of the plaintiff class members didn't already have an expectation of privacy, Viacom's notice created an expectation of privacy. Viacom's violation of that trust by surreptitiously collecting data from children could be considered highly offensive under the applicable law.

## Summary

An IP address has been likened to a computer's fingerprint. If a statute identifies an IP address or other static assigned number as PII, that number is a great starting point to identify a user. For example, under COPPA and HIPAA, an IP address is as high on the spectrum of PII as a user's first and last name. The rationale behind the ranking of an IP address in these statutes is that sometimes it is reasonable that an IP address can lead you to the user. Who's looking for you also matters. It is reasonable that Google, using third-party cookies, can reasonably use your IP address to identify you.



Sometimes an IP address can only identify a computer, i.e., it cannot "reasonably" be used to identify you. Without a subpoena or some alternate means of creating a mosaicked identity, you may have to resort to battling "John Doe" until a subpoena grants you the right to retrieve additional information about the IP address. In these instances, IP addresses are not considered to be PII. At the end of the day, you have found a computer. Good job.

---

<sup>13</sup> *Hennessy v. Coastal Eagle point Oil Co.*, 609 A.2d 11, 17 (N.J. 1992 (citing Restatment (Second) of Torts § 652B (1977))).

## What did we learn?

- Don't over sell your privacy policy. Viacom faces potential liability because it violated its own privacy notice to parents.
- Do the right thing. Don't get information from children under the age of 13 that is defined as PII under any privacy law without parental consent. These days there are few things about which 90 percent of Americans agree — Viacom's actions on the Nick Sites are considered to be highly offensive.
- Now that you know that sometimes children's browsing history, IP address and other information can be collected through third-party cookies without parental consent, educate your children. The Federal Trade Commission provides guidance on helping children distinguish between ads and entertainment: <https://www.common sense media.org/website-reviews/admongo>.
- Understand that a trade-off for having the world at your fingertips may mean sharing your computer's fingerprint with inquiring minds.

Stay safe.



### **Jane E. Brown**

Jane is Counsel to the Firm at Lane Powell and focuses her practice on both transactional matters and civil litigation. As former in-house counsel, she is skilled in focusing and quickly assessing the circumstances, alerting clients to potential revenue streams and liabilities, and working toward cost-effective resolutions. Jane's litigation experience includes representation of clients in highly regulated industries. She assists clients with the development and maintenance of privacy policies, drafting provisions to protect privacy, and complying with state, federal and international regulation regarding cybersecurity and data breach response. She can be reached at 206.223.7126 or [brownje@lanepowell.com](mailto:brownje@lanepowell.com).

1.800.426.5801

[lanepowell.com](http://lanepowell.com)

This is intended to be a source of general information, not an opinion or legal advice on any specific situation, and does not create an attorney-client relationship with our readers. If you would like more information regarding whether we may assist you in any particular matter, please contact one of our lawyers, using care not to provide us any confidential information until we have notified you in writing that there are no conflicts of interest and that we have agreed to represent you on the specific matter that is the subject of your inquiry.

Copyright © 2016 [Lane Powell PC](http://Lane Powell PC)