Client Update

New Decision Confirms Narrow Meaning of "Personally Identifiable Information" Under Video Privacy Statute

The Ninth Circuit recently dealt another blow to attempts to expand corporate liability under the Video Privacy Protection Act ("VPPA"). In *Eichenberger v. ESPN*, the Ninth Circuit affirmed the district court's dismissal of a VPPA class action that accused ESPN of disclosing personal information in the form of a device serial number. The Ninth Circuit held that disclosures of personally identifiable information ("PII") are only actionable if they "readily permit an ordinary person to identify" a specific individual, which device numbers don't do.

VPPA prohibits a "video tape service provider" from disclosing "information which identifies a person as having requested or obtained specific video materials or services."[1] VPPA was enacted in 1987, after the clerk at a neighborhood video store handed a reporter the tape rental history of Judge Robert Bork. Congress provided for liquidated damages of $2,500 per violation, plus attorneys' fees—amounts that would yield eye-popping damages at Internet scale. The plaintiffs' bar thus has filed class actions against a host of online video companies.

These cases all rest on a simple premise: The company providing an online video to you typically also provides information about the viewing session to third parties, like advertising service companies and analytics firms. This information usually takes the form of an anonymous number string, such as the device identifier on your smartphone. Plaintiffs argue that sharing these anonymous number strings is the digital equivalent of the video store clerk handing over a hard copy of Judge Bork's tape rental history.

Whether plaintiffs are right depends on whether the number string associated with your viewing session "identifies a person" within the meaning of VPPA. Put another way: When Video Streaming Company tells Analytics Firm that it has just sent video XYZ to device number 123456, does that "identify" John Smith as the owner of the device? Plaintiffs have argued that it

[1] 18 U.S.C. § 2710(a)(3).

does, because there are various ways of connecting the dots between device identifier 123456 and John Smith.

At issue in *Eichenberger* was the device identifier of a Roku box. The Ninth Circuit said that the identifier alone wasn't enough under VPPA: a Roku device identifier "*cannot* identify an individual unless it is combined with other data." Indeed, the Ninth Circuit emphasized that only a "complex" process "to link an individual's Roku device number with other identifying information derived from an enormous amount of information collected from a variety of sources" would allow a third party to identify an individual. That meant that the Roku identifier alone wasn't PII.

The Ninth Circuit joined the Third Circuit, in *In re Nickelodeon Consumer Privacy Litigation*, which held that PII "means the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior."

Both *Eichenberger* and *Nickelodeon* distinguished a First Circuit case, *Yershov v. Gannett Satellite Info. Network, Inc*. There, the First Circuit held that an iPhone device ID, when disclosed along with GPS coordinates, was PII under VPPA. For now, the still-emerging law in this area seems clear: anonymous number strings are not PII "without more," and *Yershov* is an outlier that went plaintiffs' way because of the identifying power of GPS data.

Eichenberger was not a complete success for the defense: The Ninth Circuit joined others in holding that VPPA plaintiffs have standing even though the disclosures did not cause them real-world harm. Courts have reasoned that VPPA codifies a substantive right to privacy, and that this is constitutionally sufficient to create a case or controversy under Article III granting plaintiffs standing. The Supreme Court's 2016 *Spokeo* decision, which created a test for standing in statutory privacy cases, has been of little help to VPPA defendants thus far.

This area of the law is evolving rapidly. Some best practices include:

- **Know that you're a potential VPPA defendant**. Compliance starts with awareness of risk. Companies whose core business involves video streaming (like Netflix, Hulu, ESPN, CNN and Viacom) have all been hit with VPPA suits. But in a world where virtually all companies provide some form of streaming video on their websites, everyone's a target.
- **Know what information you're passing to which third parties**. This isn't always easy to tell; the ecosystem of online video delivery is complex and involves a host of players. Consider how the flow of information to third parties can be kept to a minimum. Then revisit your processes regularly: the flow of information may be different a month or a year from now.
- **Watch this space**. VPPA litigation remains ongoing. The narrow definition of PII adopted in *Eichenberger* and *Nickelodeon*, while clearly correct, could evolve. Even today, that

definition does not necessarily apply in other contexts. The FTC staff, for example, takes the view that "data that is reasonably linkable to a consumer or a consumer's device is personally identifiable." The staff thus cautions that companies should avoid making broad statements in their privacy policies that they are not collecting PII. Likewise, EU law may treat IP addresses and other anonymous digital data as PII in contexts where U.S. law would take a different approach.

* * *

We would be pleased to discuss these issues with our clients and friends.

NEW YORK

Jeremy Feigelson
jfeigelson@debevoise.com

Christopher S. Ford
csford@debevoise.com

Neelima Teerdhala
nteerdhala@debevoise.com