ROPES & GRAY

ALERT

Privacy & Cybersecurity

December 22, 2017

Ninth Circuit Weighs In On Scope of Identifiable Information under VPPA

Attorneys
Heather Egan Sussman
Douglas H. Meal
James S. DeGraw
Seth C. Harrington
Mark P. Szpak
Michelle Visser
David T. Cohen

On November 29, 2017, the Ninth Circuit added to an existing circuit split that has emerged regarding the definition of "personally identifiable information" under the Video Privacy Protection Act (VPPA). The Ninth Circuit affirmed the dismissal of a class action after construing the term to include only information that enables an "ordinary person" to identify an individual. *Eichenberger v. ESPN, Inc.*, No. 15-35449, 2017 WL 5762817 (9th Cir. Nov. 29, 2017). This interpretation puts the Ninth Circuit at odds with the First Circuit, which last year adopted a more expansive definition of "personally identifiable information" that potentially extends the reach of the VPPA to far more online tracking activity. (Our Alert on the First Circuit's decision is here.) While the Ninth Circuit's *Eichenberger* decision is helpful for online actors concerned about the potential for class actions and large-scale statutory damages under the VPPA, the circuit split underscores the ambiguity in the VPPA, and online actors should not necessarily view the Ninth Circuit's decision as a green light or the last word. In addition, and potentially just as challenging, the VPPA remains only part of the overlapping and increasingly complex regulatory environment for online tracking, including developments at the Federal Trade Commission and in the European Union's upcoming General Data Protection Regulation (GDPR) and ePrivacy Regulation.

The VPPA prohibits "video tape service provider[s]" from knowingly disclosing "*personally identifiable information* concerning *any consumer*" without a particularly onerous form of consent. 18 U.S.C. § 2710(b)(1)-(2) (emphasis added). "[P]ersonally identifiable information" in turn "includes information which identifies a person as having requested or obtained specific video materials or services." § 2710(a)(1). While the VPPA was originally passed in 1988 to address disclosure of video rental history by brick-and-mortar video rental stores, it has become increasingly attractive to plaintiffs' lawyers and others objecting to video data-sharing practices because of its damages provisions. A court may award damages to any person aggrieved by a violation of the Act, that are "not less than liquidated damages in an amount of $2,500" in addition to punitive damages and attorneys' fees. 18 U.S.C. § 2710(c)(2). And those circuit courts that have considered the question, including the Ninth Circuit here, have held that a violation of the VPPA's substantive provisions is itself sufficient for Article III standing.

Courts have struggled with defining "personally identifiable information" for purposes of the VPPA. Last year, in *Yershov v. Gannett Satellite Info. Network, Inc.*, 82 F.3d 482 (1st Cir. 2016), the First Circuit held that mobile device GPS data constituted "personally identifiable information" when that information was disclosed to Adobe for analytics and marketing because the data was "*reasonably and foreseeably likely*" to identify the user. *Id.* at 486 (emphasis added). A Third Circuit decision following *Yershov* took a narrower approach to analogous data, finding that an IP address, browser settings, and device ID were not "personally identifiable information" when disclosed to a marketing and analytics provider because that information would not "*permit an ordinary person to identify*" a specific individual. *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 290 (3d Cir. 2016) (*cert. denied*).

In the Ninth Circuit's recent *Eichenberger* decision, the court considered whether a Roku device identifier in conjunction with a user's video viewing history was "personally identifiable information" under the VPPA. The court examined the approaches taken by the First and Third circuits, and adopted the Third Circuit's narrower construction of "personally identifiable information," holding that it means information that would "permit an

ordinary person" to identify an individual. Although rejecting the First Circuit test, the Ninth Circuit attempted to reconcile its holding with that of the First Circuit, suggesting that geolocation data may be identifiable to an ordinary person.

The distinction between the two tests is that the "ordinary person" test is a narrower, objective test – it does not rely on the recipient's capabilities. By contrast, the "*reasonably and foreseeably likely*" test is contextual. Applying the latter, the First Circuit accounted for the capability of Adobe to combine the disclosed data with other data in a way that may have allowed Adobe to identify the plaintiff. Under the "ordinary person" test, these capabilities and other data sources are irrelevant to whether information is personally identifiable. While the Third and Ninth circuits' adoption of the narrower approach presents a potential hurdle for plaintiffs in those circuits, the risk of litigation remains heightened in the First Circuit, which has adopted the broader test, and in the other circuits that have not addressed the issue.

Other sources of risk in this area remain as well. For instance, the FTC has in several enforcement actions and other statements indicated that it takes a more expansive view of what information is considered personally identifying or sensitive information about individuals. That information, according to the FTC, can include device identifiers and analogous data. Last year, for instance, the FTC and the New Jersey Attorney General's joint enforcement action against Vizio included allegations that Vizio shared consumers' video viewing habits, and that device identifiers and IP addresses rendered that information personally identifiable. The complaint referred to this data as "sensitive television viewing activity" and alleged that the sharing of such information without consent was both an unfair and deceptive trade practice. Vizio did not challenge the FTC's untested assertion, and the action resulted in a $2.2 million settlement. The FTC has also issued a cross-device tracking staff report, recommending transparency, choice, and consent in similar contexts.

The "ordinary person" test adopted by the Third and Ninth circuits also diverges from the meaning of "personal data" under the GDPR, which requires consideration of "all the means reasonably likely to be used . . . by the controller *or by another person* to identify the natural person *directly or indirectly*." GDPR, Recital 26 (emphasis added). Thus, structuring data collection and sharing arrangements in the video context likely will remain a complex affair for companies operating internationally.

The potential for statutory penalties available under GDPR, the burdensome nature of the remedies sought by the FTC (compliance programs, monitoring and in some cases monetary relief), and the availability of statutory damages under the VPPA underscore the value of proactively assessing and mitigating risk in advance, ideally with the assistance of counsel familiar with this area of the law. And, in the face of a class action or regulatory investigation, companies should engage counsel familiar with privacy and data security concerns broadly.

For more information regarding the VPPA or cross-device tracking, or to discuss data risk management practices generally, please feel free to contact Heather Sussman, Doug Meal, Jim DeGraw, Seth Harrington, Mark Szpak, Michelle Visser, David Cohen, or another member of Ropes & Gray's leading privacy & cybersecurity team.