Bloomberg BNA

Privacy and Security Law Report®

Video Privacy Protection Act

This article explores how personally identifiable information has been defined in leading Video Privacy Protection Act actions and looks at how concerns over the potential sensitivity of geolocation information may alter how courts handle PII. Companies must pay close attention to exactly what information they transmit to third parties—especially when that information relates to a consumer's precise geolocation, the authors write.

The VPPA and PII: Is Geolocation Another Anonymous Identifier?

BY D. REED FREEMAN AND JOSEPH JEROME

Although litigation under the Video Privacy Protection Act (VPPA) has exploded in recent years, plaintiff's attorneys have had limited success on the merits, typically because courts have shown restraint in applying the law to modern online streaming technologies. Moreover, courts have generally taken a narrow view with respect to what constitutes personally identifiable information (PII) under the statute.

D. Reed Freeman is a partner at WilmerHale LLP in Washington and co-chair of the Cybersecurity, Privacy and Communications practice.

Joseph Jerome is an associate at WilmerHale in Washington and a member of the Cybersecurity, Privacy and Communications practice.

A recent decision by the U.S. Circuit Court of Appeals for the First Circuit, however, not only throws into question how PII may be understood, but also threatens to create a circuit split should any other circuit court tackle whether the definition of PII includes anonymous identifiers, geolocation data and elements of data that are sometimes passed from a streaming service to third parties, such as analytics providers. This article explores how PII has been defined in leading VPPA actions and looks at how concerns over the potential sensitivity of geolocation information may alter how courts interpret PII under the VPPA in the future.

With limited exceptions, the VPPA imposes liability—and statutory damages of $2,500 per violation—on any ''video tape service provider'' (VTSP) that knowingly discloses PII about a consumer without the consumer's consent. 18 U.S.C. § 2710(b). Online streaming services such as Netflix Inc., Hulu Inc., and others have come to be considered VTSPs, and as digital data has entered the fray, a key question has been what, if any, of the information they pass to third parties is PII under the VPPA. Unfortunately, the statute defines PII only as ''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)(3). As the First Circuit recently noted, this definition is both awkward and unclear *Yershov v. Gannett Satellite Info. Network*, No. 15-1719, 2016 BL 136751 (1st Cir. Apr. 29, 2016) (15 PVLR 954, 5/9/16). Courts have repeatedly struggled to understand the scope of information encompassed by PII and how precisely this information must identify a person. *E.g. Robinson v. Disney Online*, No. 14-CV-04146-RA, 2015 BL

 ISSN 1538-3423

344231 (S.D.N.Y. Oct. 10, 2015) (Opinion & Order) (14 PVLR 1935, 10/26/15).

I. *In re Hulu Privacy Litigation* Sets the Stage

Perhaps because of the law's limited scope and applicability solely to the disclosure of audio visual materials, there were very few cases challenging disclosures under the VPPA for the first two decades following its passage in 1988. Beginning in 2011, however, plaintiffs began advancing new theories to broaden the law's scope to apply to online cookies and other user identifiers that are frequently shared with analytics companies, social media services and third-party advertisers. With *In re Hulu Privacy Litigation* in 2012, a Northern District of California court became the first to address how the VPPA applies to online streaming video, and the *Hulu* case has become foundational in any analysis of what is PII under the VPPA (11 PVLR 1287, 8/20/12).

Plaintiffs alleged that Hulu improperly disclosed unique customer identifiers to a marketing analytics firm and, importantly, disclosed video viewing history to a social network service using the service's own first-party user IDs. *In re Hulu Privacy Litig.*, No. C 11-03764 LB, 2014 BL 120236 (N.D. Cal. Apr. 28, 2014) (13 PVLR 795, 5/5/14). Hulu argued that it was not liable for these disclosures because it never combined or linked the user IDs to identifying data such as a person's name or address, but the court found that individuals could be identified in many different ways: by a picture; by pointing; by an employee number; by the station or office or cubicle where one works; or by simply telling someone what ''that person'' rented. *Id.*

Courts have generally taken a narrow view with respect to what constitutes personally identifiable information.

The court held that the VPPA did not require the disclosure of a name but rather prohibited ''the identification of a specific person tied to a specific transaction.'' *Id.* The court further noted that a unique anonymized ID alone is not PII in and of itself, but that circumstances could render it non-anonymous, and thus the equivalent of the identity of a specific person. *Id.*

In other words, the court held that context matters. For example, the court found that disclosing unique user IDs and watch pages to the analytics firm comScore was not a disclosure of PII because there was no evidence comScore actually used this information to access Hulu users' profile pages or otherwise obtain their names. The court also addressed the disclosure to comScore of comScore's own user ID cookies, which allowed comScore to recognize and track users online. The court recognized both that ''there may be substantial tracking that reveals a lot of information about a person'' and that the cookies could show ''someone's consumption relevant to an advertiser's desire to target ads to them,'' but because this tracking did not reveal ''an identified person and his video watching,'' it was not a VPPA violation. *Id.*

On the other hand, the court suggested that the disclosure of Facebook's own user IDs back to Facebook itself along with Hulu viewing history *could* constitute disclosure of PII under the VPPA. The court stated that a ''Facebook User ID is more than a unique, anonymous identifier. It personally identifies a Facebook user.'' *Id.* The court also highlighted the fact that ''a Facebook user – even one using a nickname – generally is an identified person on a social network platform'' and thus, a Facebook User ID could easily identify ''the Hulu user's actual identity on Facebook.'' *Id.*

II. *Yershov v. Gannett*: Anonymous Device Identifier Plus More

With the *Hulu* case as a cornerstone, subsequent VPPA litigation has turned on whether certain types of information—or combinations thereof—can amount to PII. As discussed below, the majority of courts have been skeptical of these efforts, but the First Circuit, in *Yershov v. Gannett*, has embraced the notion that anonymous identifiers in connection with precise geolocation information may constitute PII under the VPPA.

Alexander Yershov, the plaintiff, downloaded and installed the USA Today Mobile App offered by Gannett onto his Android device. He alleged that each time he viewed a video clip on the app that Gannett disclosed to an analytics third party: (1) the title of the video viewed; (2) his device's unique Android ID; and (3) the GPS coordinates of the device at the time the video was viewed. While the district court granted Gannett's motion to dismiss on the grounds that Yershov was not a ''subscriber'' protected under the VPPA, it did hold that the information disclosed by Gannett could fit under the VPPA's definition of PII. The U.S. Court of Appeals for the First Circuit not only found that Yershov could be considered a subscriber, but more importantly, it also agreed with the district court's broad definition of PII.

The First Circuit reiterated that ''[m]any types of information'' could be used to ''easily identify a person.'' It even used a football metaphor, suggesting that whenever a football referee announces a violation by ''No. 12 on the offense,'' anyone in the stadium ''with a game program knows the name of the player who was flagged.'' The court appeared to suggest that the combination of device identifier and GPS coordinates presented a similar scenario. *Id.* It hypothesized that disclosing that a person had viewed 146 videos at just two sets of GPS coordinates would ''enable most people to identify what are the likely home and work addresses of the viewer.'' *Id.* According to the court, disclosing this information to a marketing analytics company effectively could give the third party ''the 'game program,' so to speak, allowing it to link the GPS address and device identifier information to a certain person by name, address, phone number, or more.'' *Id.* at 8-9.

  PVLR ISSN 1538-3423

Part of the reason personally identifiable information has been so cabined is due to an effort by these courts to establish some limiting principle under the Video Privacy Protection Act.

Further, the First Circuit appears to have shifted what constitutes ''knowingly'' disclosing PII under the VPPA. Liability under the VPPA only attaches where a VTSP ''knowingly discloses'' PII without consent, (18 U.S.C. § 2710(b)(1)) and the *Hulu* case established a high standard for plaintiffs to meet in order to prove a ''knowing'' disclosure. *In re Hulu Privacy Litig*., 86 F. Supp. 3d 1090, 1098 (N.D. Cal. Mar. 31, 2015). There, the court ultimately held that Hulu did not ''knowingly'' send PII because the plaintiffs had provided no evidence that Hulu was aware that Facebook might connect separate data points. In contrast, here the First Circuit held that the linkage of device identifiers, location information, and identity was ''both firm and readily foreseeable to Gannett.'' *Id.* at 9. While it acknowledged that that at some point the linkage of information to identity could become too uncertain, it found that the plaintiff plausibly alleged that Gannett disclosed information ''reasonably and foreseeably'' likely to reveal Yershov's identity. *Id.*

III. The Narrower Majority Rule

At first glance, the First Circuit's decision in *Yershov* stands as an outlier. The majority of districts courts have embraced a far narrower definition of PII under the VPPA as information which ''must, without more, itself link an actual person to actual video materials.'' *In re Nickelodeon Consumer Privacy Litig*., 2014 BL 186702 at *11 (D.N.J. July 2, 2014). *Nickelodeon* is illustrative of the full scope of this majority rule.

The plaintiffs in *Nickelodeon* had alleged that Viacom Inc. disclosed to Google a wealth of information about video streaming on Nick.com in order to target advertising. A District of New Jersey court dismissed the case, holding that anonymous usernames, internet protocol (IP) addresses, browser settings, unique device identifiers, operating systems, screen resolutions, browser versions and detailed URL requests and video materials requested and obtained—either individually or aggregated—''could [not] without more serve to identify an actual, identifiable plaintiff.'' *Id.* The court even went so far as to suggest that IP-derived geolocation information could not be used to identify a specific individual.

Other decisions have been similarly supportive of companies' ability to disclose anonymous information. In a case decided one week before *Yershov*, a Northern District of Georgia court held in *Perry v. CNN* that the disclosure by the CNN Inc. App of a static Media Access Control (MAC) address and a complete record of the user's activities could not qualify as PII. *Perry v. Cable News Network, Inc*., No. 1:14-CV-02926 (N.D. Ga. Apr. 20, 2016) (13 PVLR 1813, 10/20/14). That court was bound by a decision by the U.S. Court of Appeal for the Eleventh Circuit, which had previously appeared to endorse the notion that the VPPA emphasizes disclosure and ''not comprehension by the receiving person.'' *Ellis v. Cartoon Network, Inc*., No. 1:14-CV-484-TWT, 2014 BL 283139, at *3 (N.D. Ga. Oct. 8, 2014), aff'd on other grounds, 803 F.3d 1251 (11th Cir. 2015) (13 PVLR 1813, 10/20/14). As a result, violations of the VPPA were impossible where a third party needed to ''collect information from other sources'' in order to use Android IDs and viewing histories to identify a plaintiff. *Id.* Similarly, other courts have found allegations that third parties ''used information gathered from other sources to link plaintiff's Roku device serial number and the record of what videos were watched to plaintiff's identity'' failed to state a claim for disclosure of PII under the law. *Eichenberger v. ESPN, Inc*., C14-463, 2015 BL 134605 (W.D. Wash. May 7, 2015) (Order) (14 PVLR 906, 5/18/15). In general, any disclosure that would require a third party ''to take extra steps'' in order to identify a consumer would not violate the VPPA under this line of reasoning. *Eichenberg* 2015 BL 134605, at *5.

The *Yershov v. Gannett* decision highlights the ongoing need for companies to remain vigilant of practices and information sharing that could give rise to Video Privacy Protection Act claims.

Part of the reason PII has been so cabined is due to an effort by these courts to establish some limiting principle under the VPPA. The *Nickelodeon* court conceded that much of this sort of information ''might one day serve as the basis of personal information after some effort on the part of the recipient, but the same could be said for nearly any type of personal information.'' *Nickelodeon* at *12. Instead, the VPPA required ''a more tangible, immediate link.'' *Id.* In *Robinson v. Disney Online*, a Southern District of New York court warned that a limitless definition of PII would also undermine the VPPA's ''knowing'' disclosure require since ''if virtually all information can, in the end, be identifying, it is hard to conceive of a case in which a disclosure would not be knowing.'' *Robinson v. Disney Online*, 2015 BL 344231, at 5 (S.D.N.Y. Oct. 10, 2015) (Opinion & Order). That court held that the ''most natural reading of PII'' is that disclosed information ''must itself do the identifying that is relevant for purposes of the VPPA'' and not be akin to disclosures ''plus other pieces of information collected elsewhere.'' *Id.*

IV. Geolocation as Hulu's ''Correlated Look-Up Table''

Yershov may stand for the proposition that geolocation information is the something ''more'' that courts have been looking for since *Hulu*. While the First Circuit is currently alone in its interpretation of PII to include precise geolocation information, the circumstances of Yershov's allegations are unique in that he alleges that Gannett shared GPS information. That allegation is the one significant difference between *Yershov* and the nearly identical dispute in *Perry v. CNN*, which

arrived at a completely opposite conclusion. From the Supreme Court on down, the courts have become increasingly aware of the implications of location tracking, (*United States v. Jones*, 132 S. Ct. 945, 565 U.S. (2012)) and the First Circuit's decision in *Yershov* appears to voice a generalized concern regarding the sensitivity of precise geolocation information about an individual.

Though courts have been consistently hesitant to find information that is, in and of itself, anonymous to be PII under the VPPA, it is important to recall that the *Hulu* court initiated the notion that anonymous information could become ''the equivalent of the identification of a specific person'' in some contexts. *In re Hulu Privacy Litig*., 2014 BL 120236, at *13. It further cautioned that context matters where the information being shared could permit a ''mutual understanding that there has been a disclosure'' of PII. *In re Hulu Privacy Litig*., 86 F. Supp. 3d 1090, 1097 (N.D. Cal. 2015). As a result, a VTSP ''could not skirt liability under the VPPA, for example, by disclosing a unique identifier and a correlated look-up table.'' *In re Hulu Privacy Litig* 2014 BL 120236, at *12. With respect to sharing Global Positioning System (GPS) information, the First Circuit appears to be embracing the suggestion that geolocation data effectively provides the equivalent of an identity look-up table, and they are not alone in that regard.

The Federal Trade Commission (FTC) has repeatedly emphasized that it views data as ''personally identifiable'' wherever it can be ''reasonably linked to a particular person, computer, or device.'' While the FTC has suggested that this standard might be met by device identifiers, MAC addresses, and other persistent identifiers, it has also stated that ''location information is particularly useful for uniquely identifying (or re-identifying) individuals.''

That said, it is unclear how the mere provision of an anonymous Android ID, GPS information, and a record of videos being watched can identify a specific person without ''extra steps'' called for by *Ellis*, *Eichenberger* and *Locklear v. Dow Jones* being taken by a third party. The First Circuit cites no precedent to explain why geolocation data is different, and it provides little insight into how and when geolocation information can be construed to be PII. Interestingly, as if to avoid setting too broad a precedent, the court also quickly backpedaled, insisting that its holding should not be viewed ''quite as broad as [its] reasoning suggests.''

It is too early to say to what extent *Yershov* will influence other VPPA actions. A different panel of judges easily could have arrived at a different conclusion, but after the First Circuit declined to grant a rehearing *en banc*, we now have one circuit court firmly on the record as to what may constitute PII under the VPPA. If nothing else, the decision highlights the ongoing need for companies to remain vigilant of practices and information sharing that could give rise to VPPA claims. Companies must pay close attention to exactly what information they transmit to third parties—especially when that information relates to a consumer's precise geolocation.

  PVLR ISSN 1538-3423