Bloomberg BNA

Privacy and Security Law Report®

Video Privacy Protection Act

Over two decades after passage, the Video Privacy Protection Act was resurrected by the plaintiffs' class action bar lured by the availability of substantial statutory damages. Given the uncertainty regarding the contours of some aspects of the VPPA as applied to modern technology, and the lure of potentially hefty statutory damages, VPPA litigation is likely to continue in the future, the authors write.

Teaching an Old Law New Tricks: The 1988 Video Privacy Protection Act in the Modern Era

BY JOSHUA JESSEN AND PRIYANKA RAJAGOPALAN

Joshua Jessen is a partner at Gibson, Dunn & Crutcher LLP in Irvine, Calif. and is a member of the firm's Privacy, Cybersecurity and Consumer Protection Group, Intelelctual Property Group and Health Care and Life Sciences Group.

Priyanka Rajagopalan is an associate at Gibson Dunn & Crutcher LLP in Palo Alto, Calif. and is a member of the firm's Litigation Practice Group and Privacy, Cybersecurity and Consumer Protection Group.

Introduction

The Video Privacy Protection Act (VPPA) was enacted in 1988 in a pre-internet era. The VPPA made it unlawful for ''video tape service providers''—at the time brick and mortar establishments—to disclose the records of ''prerecorded video cassette tapes or similar audio visual materials'' requested or obtained by their customers, without consent. The statute largely sat dormant for many years. But over two decades later, it was resurrected by the plaintiffs' class action bar, which, lured by the availability of substantial statutory damages ($2,500 per violation), began using the statute to challenge the information sharing practices of online providers of video content (i.e., certain websites and mobile applications).

The information sharing practices of these modern entities (which tend to involve the disclosure of anonymous identifiers, not personally identifiable information) have been a far cry from the conduct that motivated passage of the VPPA, and most of the lawsuits claiming that these practices violate the VPPA have rightly failed to gain traction. But the plaintiffs' bar has not given up, and there remains uncertainty over the application of some aspects of the VPPA in the context of many modern technologies. Some recent cases illustrate the difficulty courts face in applying a pre-internet statute to the practices of certain online and mobile platforms. As a result, online providers of video content

 ISSN 1538-3423

should review their data collection and sharing practices to avoid becoming ensnared in a costly class action lawsuit. This article explores the VPPA's history and contours, its applicability in the modern context, and its likely future in the courts.

A Brief History of the VPPA

The VPPA finds its origins in a newspaper story with some unintended consequences. At the end of September 1987, during Judge Robert Bork's (ultimately ill-fated) Supreme Court nomination hearings, Michael Dolan, a Washington, D.C. newspaper reporter, obtained a list of 146 video tapes Judge Bork and his family had rented from his neighborhood video rental store and published that list in a local newspaper in an article titled ''The Bork Tapes.''

In a twist Dolan likely did not expect, Judge Bork suffered no real embarrassment, but there was widespread congressional outrage over this perceived invasion of privacy. In the spring of 1988, Senators Patrick Leahy (D-Vt.), Paul Simon (D-Ill.), and Charles Grassley (R-Iowa) introduced Senate Bill 2361, which would eventually become the VPPA. Grassley explained that the purpose of the bill was to prevent video stores from perpetuating such leaks and ''disclosing their customers' names, addresses and specific video tapes rented or bought by the customers.'' 134 Cong. Rec. S16312-01, 1988 WL 177971 (Oct. 14, 1988). The bill's focus on linking identified individuals to their specific video-viewing records was clear; the Senate Judiciary Committee Report explained that ''personally identifiable information'' (PII), which could not be disclosed with a customer's consent under the bill, was ''intended to be transaction-oriented''—i.e., ''it is information that identifies a *particular* person as having engaged in a *specific transaction* with a video tape service provider.'' *See* S. REP. 100-599, 1988 (emphasis added).

The information sharing practices of modern entities (involving the disclosure of anonymous identifiers, not personally identifiable information) have been a far cry from the conduct that motivated passage of the Video Privacy Protection Act.

The legislative interest in preventing personal embarrassment was an ongoing theme. For instance, the Judiciary Committee's report quoted testimony from counsel for the ACLU that ''[a]lthough Judge Bork recently joked about how embarrassed he is to have the world learn that he watches dull movies, imagine if his confirmation had been doomed by the revelation of more unsettling viewing habits.'' *Id*. The report also quoted a congressman who sponsored the first Video Privacy bill: ''There's a gut feeling that people ought to be able to read books and watch films without the whole world knowing. Books and films are the intellectual vitamins that fuel the growth of individual thought. The whole process of intellectual growth is one of privacy—of quiet, and reflection. This intimate process should be protected from the disruptive intrusion of a roving eye.'' *Id*. The bill passed both houses of Congress and was signed into law by President Reagan in November 1988.

In 2012, after more than twenty years of relative inactivity, Representative Robert Goodlatte (R-Va.) led a bipartisan effort to amend the statute to ''reflect the realities of the 21st century,'' which Netflix Inc. and other video content providers supported. The Video Privacy Protection Act Amendments Act of 2012 was signed into law by President Obama in January 2013 (12 PVLR 76, 1/14/13). The amendments acknowledged the impact of the internet and amended the VPPA to make it easier for consumers to share their movie preferences online. S. Rep. No. 112-258, at 2-3 (2012) (''This update to the law will allow American consumers to continuously share their movie or television preferences through social media sites.''). The amendment removed the requirement that video tape service providers obtain written consent from users every time a user's viewing choice was disclosed, and instead allowed for a provider to obtain a user's consent online (''through an electronic means using the Internet'') for a set period of up to two years.

The Statute

The VPPA ostensibly governs the same activity that motivated its passage: video stores disclosing lists of the videos rented, sold or delivered to a particular customer without consent. The statute regulates ''video tape service providers,'' defined as ''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.'' 18 U.S.C. § 2710(a)(4). Subject to certain exceptions, it prevents such video tape service providers from ''knowingly disclos[ing], to any person, personally identifiable information concerning any consumer of such provider'' without consent. *Id.* § 2710(b)(1). And, keeping with the initial purpose of the statute, it defines ''personally identifiable information'' as ''includ[ing] information which *identifies a person* as having requested or obtained *specific video materials or services* from a video tape service provider.'' *Id.* § 2710(a)(3) (emphasis added). The statute creates a private right of action that allows for ''liquidated damages'' of $2,500 per violation. *Id.* § 2710(c).

As a result of the 2012 amendments to the VPPA, video tape service providers may now obtain up-front, online consumer consent to share video viewing information with third parties. *See* Pub. L. 112-258 (altering the consent requirements to ''clarify that a video tape service provider may obtain a consumer's informed, written consent [to disclose PII] on an ongoing basis and that consent may be obtained through the Internet''). As a result, video tape service providers can now obtain advance online user consent for all PII transmissions for up two years, or until the user withdraws their consent. 18 U.S.C. § 2710(b)(2)(B). This option must be provided separately from any other statement of the user's legal or financial obligations, and the user must be able to opt out anytime or on a case-by-case basis.

  PVLR ISSN 1538-3423

The Video Privacy Protection Act amendments acknowledged the impact of the internet and amended the VPPA to make it easier for consumers to share their movie preferences online.

The VPPA's Applicability to Websites and Mobile Applications That Provide Video Content

''Video Tape Service Providers''

Courts generally have found that online streaming video providers, such as Netflix and Hulu LLC, qualify as ''video tape service providers'' under the statute. *See Mollett v. Netflix, Inc.*, 5:11-CV-01629-EJD, 2012 BL 210456 (N.D. Cal. Aug. 17, 2012) (11 PVLR 1341, 9/3/12); *In re Hulu Privacy Litig.*, C 11-03764 LB, (N.D. Cal. Aug. 10, 2012) [hereinafter ''*Hulu*''] (11 PVLR 1287, 8/20/12). Given the nature of these companies' businesses, these holdings perhaps are not surprising. But plaintiffs' attorneys also have filed a string of VPPA lawsuits against online platforms that provide many types of content (only some of which are video content) and whose businesses are not analogous to the video stores of the 1980s. *See, e.g.*, *Perry v. Cable News Network, Inc.*, No. 14-cv-1194 (N.D. Ill.); *Ellis v. The Cartoon Network, Inc.*, No. 14-cv-484 TWT, 2014 BL 283139 (N.D. Ga.) (13 PVLR 1813, 10/20/14); *Locklear v. Dow Jones & Company, Inc.*, No. 14-cv-744 2015 BL 34428 (N.D. Ga.) (14 PVLR 198, 2/2/15).

It is highly questionable whether these entities should be considered ''video tape service providers,'' but, at least at the pleading stage, most courts have accepted (or found it unnecessary to reach) plaintiffs' allegations that these entities qualify as ''video tape service providers.'' If future VPPA cases advance beyond the pleading stage, however, defendants who do not run businesses that are analogous to traditional video stores should consider arguing that they simply do not fit within the definition and are therefore not covered by the statute.

'Knowing Disclosure' of 'Personally Identifiable Information'

While courts have tended to credit allegations that modern defendants that provide online streaming video content are ''video tape service providers,'' they have frequently rejected plaintiffs' assertions that defendants have disclosed users' ''personally identifiable information'' as defined in the VPPA. Plaintiffs' failure here highlights the problem of attempting to map the VPPA onto modern websites and mobile apps that allow viewers to watch videos online. Specifically, many online services do not even collect, let alone disclose to third parties, their viewers' ''names and addresses'' or comparable information—i.e., the type of personal information that Grassley contemplated when introducing the bill in Congress. Instead, these providers often obtain—simply as a matter of device functionality—certain numeric identifiers, such as computer or mobile device identifiers, and may transmit this anonymous information, along with other data to a third party vendor that provides data analytics or other services.

For the most part, courts have rightly recognized that this type of disclosure is not prohibited by the VPPA, which requires knowingly transmitting information that links a *specific* person to their *specific* video request. With no plausible allegation (not to mention proof) that a website transmits (or that a third party receives) this information in a manner that links a person's identity to the videos they watched, a VPPA claim should not be viable. *See, e.g.*, *Ellis v. Cartoon Network*, 2014 BL 283139, at *3 (dismissing complaint because ''[w]ithout more, an Android ID does not identify a specific person'' and thus ''Plaintiff has not alleged the disclosure of personally identifiable information'' under the VPPA), *aff'd on other grounds*, 803 F.3d 1251 (11th Cir. 2015); *Locklear v. Dow Jones & Co.*, 2015 BL 34428, at *6 (a device serial number, without more, is not PII); *In re Nickelodeon Privacy Litig.*, MDL No. 2443, 2014 BL 186702, at *10 (D.N.J. July 2, 2014) (dismissing VPPA claim because ''PII is information which must, without more, itself link an actual person to actual video materials,'' and anonymous username, IP address, and unique device identifier do not qualify) (13 PVLR 1235, 7/14/14).

As a result, video tape service providers can now obtain advance online user consent for all personally identifiable information transmissions for up two years, or until the user withdraws their consent.

Accordingly, for VPPA liability to attach, courts generally have emphasized the need for a disclosure that clearly identifies both the person *and* their video choices in the first instance. For instance, one court explained that PII under the VPPA is ''information actually disclosed by a video tape service provider, *which must itself do the identifying . . . not information disclosed by a provider, plus other pieces of information collected elsewhere by non-defendant third-parties*.'' *Robinson v. Disney*, No. 14-4146, 2015 BL 344231 (S.D.N.Y. Oct. 20, 2015) (emphasis added) (14 PVLR 1935, 10/26/15); *see also Hulu*, C 11-03764 LB, (N.D. Cal. Mar. 31, 2015) (plaintiffs adduced no evidence that defendant knew whether or not a third party could combine a numeric identifier with video title embedded in watch page to identify a person and their video choices) (14 PVLR 603, 4/6/15); *Eichenberger v. ESPN*, No. 14-CV-00463 [Dkt. 38 at 2] (W.D. Wash. Nov. 24, 2014) (''Even if [third-party] Adobe does 'possess a wealth of information' about individual consumers, it is speculative to state that it can, and does, identify specific persons as having watched or requested specific video materials.'').

A recent appellate decision is the notable exception to this rule. In *Yershov v. Gannett*, the First Circuit acknowledged that the VPPA's definition of PII was ''awkward and unclear,'' but concluded that a plaintiff's Android ID and GPS coordinates could constitute ''PII'' under the VPPA (at least at the pleading stage). No. 15-1719, 2016 BL 136751 (1st Cir. Apr. 29, 2016) (15 PVLR 954, 5/9/16). In reaching this conclusion, the First Circuit appears to have been influenced by the plaintiff's allegation that the video provider (Gannett) knew that, when making disclosures to its analytics vendor (Adobe), Adobe had the ability to link the GPS coordinates and device identifier information to a specific person. *Id.*. The court held that, as pled in the complaint, Gannett had therefore disclosed information ''reasonably and foreseeably likely to reveal which *USA Today* videos [the plaintiff] obtained.'' *Id.* This holding represents a significant expansion of the VPPA, which by its express terms prohibits only the knowing disclosure of information that *actually* ''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).

Although most courts have found that there is no VPPA violation if ''the third party ha[s] to take extra steps to connect the disclosure to an identity,'' in light of the *Gannett* decision, companies that provide video content online and make disclosures to third parties should be wary of providing information that easily could be linked to an individual's identity. Indeed, the court in the *Hulu* case also warned that a video provider ''could not skirt liability under the VPPA, for example, by disclosing a unique identifier and a correlated look-up table'' that would allow the third party to ''look up'' numeric identifier to find the user's true identity. *Hulu*, C 11-03764 LB, 2014 BL 120236, at *12 (N.D. Cal. Apr. 28, 2014) (13 PVLR 795, 5/5/14).

Companies that deliver ''audio visual materials'' that are ''similar'' to ''prerecorded video cassette tapes'' to individuals would be well advised to review their data collection and sharing practices.

'Renters, Purchasers or Subscribers'

To state a claim under the VPPA, a plaintiff must qualify as a ''consumer,'' which the statute defines as ''any renter, purchaser, or subscriber of goods or services from a video tape service provider.'' It seems plain enough that individuals viewing free video content online are not ''renting'' or ''purchasing'' that video content. Similarly, individuals who do not register, log in, or sign up with a website or mobile application—but are merely casual viewers with no ongoing relationship with the website or app—arguably are not ''subscribers.''

Yet the issue of what constitutes a ''consumer'' under the VPPA has been a recurring issue in recent some case law, with several courts analyzing the meaning of ''subscriber.'' In the *Hulu* case, the court held that the VPPA does not limit the term to ''paid subscribers,'' and other courts have likewise agreed that payment is not a *sine qua non* of being a ''subscriber.'' But courts generally have required ''some sort of ongoing relationship'' or a ''deliberate and durable affiliation with the provider'' before an individual will be considered a ''subscriber.'' *Austin-Spearman v. AMC Network Entm't*, 98 F. Supp.3d 662, 669, 2015 BL 97917 (S.D.N.Y. 2015) (14 PVLR 658, 4/13/15). Such an ongoing relationship is often evidenced by ''an exchange between subscriber and provider whereby the subscriber imparts money and/or personal information in order to receive a future and recurrent benefit.'' *Id.*

In *Austin-Spearman*, for instance, Plaintiff alleged that AMC's website improperly disclosed her social media identifier and viewing history to a third party. The court concluded that plaintiff's sporadic ''visits to AMC's website to view various videos . . . evince no desire to forge ties with . . . AMC [because plaintiff] 'can decide to never visit the AMC website ever again—and that decision will have zero consequences, costs or further obligations.' '' *Id*. The court also rejected the plaintiff's argument that simply browsing a website while logged into a social network was sufficient to render her a ''subscriber.'' *Id.* at 670. The court explained that ''such a definition . . . sweeps so broadly as to be effectively limitless . . . rendering the 'consumer' clause superfluous.'' *Id.*

Similarly, in *Ellis*, the Eleventh Circuit held that the plaintiff's download and use of the free Cartoon Network mobile app was not sufficient to render the plaintiff a ''subscriber.'' 803 F.3d 1251 (11th Cir. 2015). While agreeing with other courts that payment was not required, the court observed that the *Ellis* plaintiff ''did not sign up for or establish an account with . . . did not provide any personal information to . . . [and] did not make any payments to Cartoon Network for use of the CN app, did not become a registered user . . . did not receive a Cartoon Network ID [or] establish a Cartoon Network profile, did not sign up for any periodic services or transmissions, and did not make any commitment or establish any relationship that would allow him to have access to exclusive or restricted content.'' *Id.* at 1257. Instead, he ''simply watched video clips on the [free] CN app''—''the equivalent of adding a particular website to one's Internet browser as a favorite''—and could ''delete the app without consequences whenever he like[d], and never access its content again.'' *Id.*

The recent First Circuit decision in *Gannett* is, however, once again the outlier—in fact, it reached the opposite conclusion from *Ellis* under largely similar facts. Plaintiffs in both cases downloaded and used free mobile apps on their Android devices, and both alleged that the apps had disclosed their Android IDs and video titles to third parties that they claimed could ascertain their identities using other independently obtained information. But unlike the Eleventh Circuit, the First Circuit concluded that the plaintiff *was* a subscriber (at least at the pleading stage) because he ''did indeed have to provide Gannett with personal information, such as his Android ID and his mobile device's GPS location at the time he viewed a video. . . access was not free of a commitment to provide consideration in the form of that information, which was of value to Gannett.'' 2016 BL 136751, at *6.

  PVLR ISSN 1538-3423

Arguing that an alleged Video Privacy Protection Act violation (without more) is insufficient to confer Article III standing has not been a successful to date.

The court also disagreed with the Eleventh Circuit and distinguished the act of downloading and using a mobile app from visiting or bookmarking a webpage on a web browser, holding that ''by installing the App on his phone, thereby establishing seamless access to an electronic version of USA Today, [plaintiff] established a relationship with Gannett that is materially different from what would have been the case had USA Today simply remained one of millions of sites on the web that [plaintiff] might have accessed through a web browser.'' *Id.*

The *Gannett* court's conclusion is questionable, but it illustrates that the metes and bounds of what it means to be a ''subscriber'' under the VPPA are still being debated, and will likely continue to be litigated in future VPPA cases.

Article III Standing

Several defendants have attempted to obtain dismissal of VPPA suits on the pleadings by arguing that an alleged VPPA violation (without more) is insufficient to confer Article III standing, but these arguments have not been successful to date. *See Hulu*, 2013 BL 359296 (N.D. Cal. Dec. 20, 2013); *Austin-Spearman*, 2015 BL 97917; *Sterk v. Redbox*, No. 13-3037, 2014 BL 300445, at *2-3 (7th Cir. Oct. 23, 2014) (13 PVLR 1836, 10/27/14).

In light of the U.S. Supreme Court's recent decision in *Spokeo v. Robins* (15 PVLR 1039, 5/23/16), however, which held that violations of a statute that are ''divorced from any concrete harm'' do not ''satisfy the injury-in-fact requirement of Article III,'' future challenges to standing in VPPA cases may be more successful. 578 U.S. _, 136 S. Ct. 1540, 1549 (2016). Indeed, the harm that motivated the passage of the VPPA—the public and widespread disclosure of an individual's movie-rental history—is so far removed from the ''harm'' alleged in recent cases that there is a serious question as to whether federal courts should continue to open the courthouse doors to plaintiffs who have suffered no real injury as a result of alleged VPPA violations. Indeed, almost all of the recent VPPA lawsuits have been of dubious merit. And while many of these cases have not survived motions to dismiss, those that have have forced companies to expend considerable resources defending against such claims—without any conceivable benefit to consumers.

Where Do We Go From Here?

Given the uncertainty regarding the contours of some aspects of the VPPA as applied to modern technology, and the lure of potentially hefty statutory damages, VPPA litigation is likely to continue in the future. Therefore, companies that deliver ''audio visual materials'' that are ''similar'' to ''prerecorded video cassette tapes'' to individuals would be well advised to review their data collection and sharing practices, as well as the consents they are obtaining from their users, to mitigate the risk of VPPA liability.

Seeking user consent is one option. As described above, the 2012 amendments to the VPPA allow video tape service providers to obtain a user's advance consent online, which is good for a period of up to two years, or until the user withdraws (whichever is earlier). 18 U.S.C. § 2710(b)(2)(B).