PAUL HASTINGS
STAY CURRENT
A CLIENT ALERT FROM PAUL HASTINGS

November 2014

The Video Privacy Protection Act: Is It the New TCPA (aka Class Action Bonanza)? A Summary of Recent Developments and Tips for Avoiding Successful Suit

BY BEHNAM DAYANIM, KEVIN P. BROUGHEL & KATHERINE J. DROOYAN

The late Judge Robert Bork is best known for his at-times controversial jurisprudence and his failed 1987 Supreme Court nomination. However, a lesser known legacy of that nomination fight, the Video Privacy Protection Act ("VPPA"), is making itself felt in a wave of class action lawsuits against media companies such as Hulu, Redbox and Cartoon Network over their alleged disclosure of consumer viewing habits.

The VPPA prohibits a video tape service provider, defined as "any person, engaged in the business … of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials," from knowingly disclosing consumers' personally identifiable information. 18 U.S.C. §§ 2710(a)(4), 2710(b)(1). The statute has been construed to apply to providers of online video streaming and similar services.

Importantly, the statute — like other statutes popular with class-action attorneys (such as the Telephone Consumer Protection Act) — does not require actual damages. Violation entitles plaintiffs to statutory damages of $2,500 per violation. 18 U.S.C. § 2710(c)(2)(A).

The VPPA was passed as a response to the newspaper publication of Judge Bork's video rental history during his confirmation hearing. However, today, in an age of social media plug-ins, web beacons and mobile apps, the sheer number of ways in which a user's personal information may be disclosed to third parties creates substantial potential vulnerability for content providers of all stripes.

We provide below a summary of some key recent court decisions involving the statute and set out suggested steps that content providers should consider proactively to reduce their exposure to successful suit.

Can They Tell If It's Really Me?

To establish a claim under the VPPA, a plaintiff must show that a provider knowingly disclosed "personally identifiable information." Personally identifiable information under the VPPA is defined as including "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).

Thus far, courts have held that information shared with third parties does not qualify as "personally identifiable" unless it "serve[s] to identify an actual, identifiable Plaintiff and what video or videos that Plaintiff watched." *In re Nickelodeon Consumer Privacy Litig.*, 2014 U.S. Dist. LEXIS 91286, at *39 (D.N.J. July 2, 2014). In *Nickelodeon*, plaintiffs visited certain children's websites operated by Viacom, one of the named defendants. Plaintiffs alleged that Viacom collected their gender, age range and video materials requested and disclosed that information to Google for purposes of targeted advertising. The *Nickelodeon* court found that such information "does not link an identified person to a specific video choice" and, therefore, did not qualify as personally identifiable information within the meaning of the statute. The court dismissed the claim. *Id*. at *40, *46-*47.

Similarly, in *Ellis v. Cartoon Network, Inc.*, 2014 U.S. Dist. LEXIS 143078 (N.D. Ga. Oct. 8, 2014), the plaintiff downloaded an application on his Android device to watch cartoon video clips. The application transmitted a complete record of his video history and Android user identification to a data analytics company without his consent. The court dismissed the VPPA claim on the basis that the Android ID did not identify a specific person and therefore no disclosure of "personally identifiable information" had occurred. *Id*. at *8-*9.

Importantly, however, at least one court has rejected a "bright-line" rule that to state a violation of the VPPA, a plaintiff must demonstrate that the disclosure be the person's actual name. *See In re Hulu Privacy Litig.*, 2014 U.S. Dist. LEXIS 59479, at *35,*43-*45 (N.D. Cal. Apr. 28, 2014) (observing "[t]he statute does not require an actual name" and denying defendant summary judgment as to disclosures to Facebook of the user's identity on Facebook even though no "actual" name was transmitted).

As a result, disclosure of a user's social-media handle or user identification may trigger liability under the act.

Consumer, Subscriber or Something Else?

Another area of litigation focus is whether plaintiffs are "consumers" under the VPPA. The VPPA defines "consumer" as a "renter, purchaser or subscriber of goods or services from a video tape service provider." 18 U.S.C. § 2710(a)(1). Defendants have posited in recent VPPA cases that plaintiffs cannot be subscribers, and therefore are not consumers, simply by visiting a website. While courts seem to accept that visiting a website alone is insufficient, the threshold for qualifying as a subscriber is low. For example, the *Hulu* court determined that the plain language of the statute did not require that plaintiffs pay for a company's services to be considered subscribers. *In re Hulu Privacy Litig.*, 2012 U.S. Dist. LEXIS 112916, at *24 (N.D. Cal. Aug. 10, 2012) ("If Congress wanted to limit the word 'subscriber' to 'paid subscriber,' it would have done so."). It was sufficient that plaintiffs alleged that "they signed up for a Hulu account, became registered users, received a Hulu ID, established Hulu profiles, and used Hulu's video streaming services." *Id*. at *23. Likewise, in *Ellis v. Cartoon Network, Inc., supra*, at *5, *6 (N.D. Ga. Oct. 8, 2014) the court approvingly cited to *Hulu* and held plaintiff was a subscriber because "[h]e downloaded the CN App and used it to watch video clips. His Android ID and viewing history were transmitted to [the data analytics company]. These facts suffice to qualify the Plaintiff as a 'subscriber,' and as such, a 'consumer.'"

Were the Disclosures Incident to the Company's Ordinary Course of Business?

The VPPA provides a safe harbor for disclosures of viewing selections and personally identifiable information that are "incident to the ordinary course of business." 18 U.S.C. § 2710 (b)(2)(E).

Ordinary course of business is defined as "debt collection activities, order fulfillment, request processing, and the transfer of ownership." 18 U.S.C. § 2710(a)(2).

Courts have grappled with how broadly to construe the ordinary course of business exception. In the recent case of *Sterk v. Redbox Automated Retail, LLC*, 2014 U.S. App. LEXIS 20505 (7th Cir. Oct. 23, 2014), the defendant operated self-service kiosks where consumers could rent DVDs and Blu-ray discs. The defendant hired a third party, called Stream, to provide customer service support to the defendant's customers. Stream was provided access to the defendant's database of customer service information in order to perform its job. Plaintiffs alleged this disclosure was not incident to the defendant's ordinary course of business because "request processing" and "order fulfillment" referred only to the kiosk's computerized response and dispensing of a selected movie after processing a customer's request. *Id*. at *14. In rejecting that argument, the *Redbox* court noted that personally identifiable information "includes information which identifies a person as having requested or obtained specific video materials *or services* from a video tape service provider." *Id*. at *13, citing 18 U.S.C. § 2710(a)(3) (emphasis added). As such, one could not reasonably interpret the statute to exclude customer service requests from "request processing." In addition, the fact that the defendant provided Stream with access to the entire customer database, even if many of those customers never had made a service request, was "meaningless" because what controlled was the fact that the purpose behind the disclosure was customer service, which fell within the defendant's ordinary course of business. *Id*. at 16.

However, activities that are not deemed central to a company's business objectives may not qualify for protection. In *In re Hulu Privacy Litig., supra*, at *20-21 (N.D. Cal. Aug. 10, 2012), the court refused to grant Hulu's motion to dismiss on the basis that factual questions existed as to whether Hulu's sharing of information with "online market research, ad network and web analytics companies" was incident to the ordinary course of Hulu's business where it was disputed if such marketing and analytic activities were in the ordinary course of Hulu's business of delivering video content to consumers.

What is a Video Tape Service Provider in This Day and Age?

Finally, recent cases have considered the question of what types of services fall within the definition of "video tape service provider" ("VTSP"). Generally speaking, courts take a liberal view of the term since, by definition, it encompasses "prerecorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710 (a)(4). For instance, in *In re Hulu Privacy Litig., supra*, at *14 (N.D. Cal. Aug. 10, 2012), Hulu contended the VPPA "only regulates businesses that sell or rent physical objects … and not businesses that transmit digital content over the Internet." In the court's view, this interpretation was unsustainable because it wrongly focused on how the content was delivered rather than the content itself. Given the legislative history of the statute and the ordinary meaning of "audio visual materials," the Court determined Hulu was a "video tape service provider" within the meaning of the statute. *Id.* at *15-*19.

However, the fact that an entity in some of its business activities may be a VTSP does not suffice. The VTSP aspect of its activities must be relevant to the claim. In *In re Nickelodeon Consumer Privacy Litig., supra*, at *27 (D.N.J. July 2, 2014), the court dismissed a VPPA claim against Google on precisely that basis. Plaintiffs alleged that "any party who is 'in possession of personally identifiable information as a direct result of the improper release of such information' is subject to VPPA liability" and, regardless, because Google owned YouTube, a provider of online video services, Google was a VTSP. *Id.* at *23, *28. In finding for Google, the court held, first, that the statute made clear that

"only VTSPs can be liable for violations of the VPPA" and, second, that "the VPPA only contemplates civil actions against those VTSP from whom 'specific video materials or services' have been requested. It is readily apparent that is not the case with Google here, nor could it ever be — YouTube videos are irrelevant to this lawsuit, which focuses exclusively on three Viacom websites and the Defendants' data collection activities in regards to those sites." *Id.* at *26, *29.

Compliance Steps Companies Should Consider

Companies providing online video streaming services and related media services must pay close attention to the types of consumer data they are disclosing and the extent to which those disclosures could open them up to class action liability. In light of the recent decisions discussed above, here are some compliance steps companies should consider to limit their exposure to VPPA liability:

- Companies should review their privacy policies and consider obtaining express consent from consumers before disclosing their personal information. Under the VPPA, consent can be obtained electronically but must be specific and separate from other legal or financial obligations. 18 U.S.C. § 2710(b)(2)(B).

- Companies should scrutinize the types of information they are collecting and disclosing to third parties. That scrutiny should include social-media plug-ins and other website and mobile integrations. Often, understanding precisely what is being shared through those channels is not immediately apparent, but information that may enable the specific identification of consumers and their content choices should trigger careful evaluation.

- Companies should carefully evaluate the purposes for which information is being disclosed and whether it legitimately may be considered part of the "ordinary course of business" such that potential liability under the VPPA may be avoided.

Paul Hastings Privacy and Data Security practice has substantial experience counseling clients on personal data privacy and information security matters. We advise clients on a full spectrum of critical issues, including privacy and security regulation and compliance in digital environments, data breach disclosure requirements, and issues specific to the financial services, direct marketing, and healthcare industries, as well as other cross-border (international) business activities. Our integrated team brings together lawyers from our Intellectual Property, Global Trade Controls, Technology, and Healthcare practices to provide cohesive and multidisciplinary legal counsel.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings lawyers:

Los Angeles

Jennifer S. Baldocchi
1.213.683.6133
jenniferbaldocchi@paulhastings.com

Andrew B. Grossman
1.213.683.6250
andrewgrossman@paulhastings.com

New York

Kevin P. Broughel
1.212.318.6483
kevinbroughel@paulhastings.com

Washington, D.C.

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com