Applying VPPA to Online Video Privacy

Jeffrey Lambe, CIPP/US

VPPA background

The scope of the VPPA has evolved from a regulation governing the brick-and-mortar world into one that reaches into the various platforms of the digital age. This change illustrates the continuing process of adapting existing law to the new frontiers of the internet. Moreover, though strides have been made, the pace of VPPA interpretation nonetheless trails behind new technological innovations.

The circumstances that led to the establishment of VPPA can be traced to President Ronald Reagan's 1987 nomination of Robert Bork to fill Justice Lewis Powell's vacancy on the United States Supreme Court. Judge Bork was a strict originalist, and many Democratic senators viewed him as too extreme to sit on the Court. Although his nomination was ultimately unsuccessful, the events surrounding it lead to a scandal that sowed the seeds for the VPPA.

During the media storm surrounding Judge Bork's nomination, a Washington D.C. newspaper obtained and published the history of his videotape rental from a local video store. Although the rental history was largely innocuous, this action led to bipartisan outrage in Congress. In 1988, Congress passed VPPA to prohibit the sharing or disclosure of consumers' video consumption history without informed written consent. In an effort to make VPPA more compatible with the digital age, Congress amended VPPA in 2012, letting consumers give consent on an opt-in basis and allowing for service providers to obtain that consent electronically.

Requirements under VPPA

VPPA is codified as 18 U.S.C. § 2710 "Wrongful disclosure of video tape rental or sale records." In relevant part, subsection (b) states: "A video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider shall be liable to the aggrieved person." The terms emphasized above are of extreme importance to the applicability of VPPA and its reach under the law — which continue to develop as technology progresses and the law evolves. Thus it is worth noting the definitions of these terms under the act.

VPPA defines a "video tape service provider" 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." With regard to "personally identifiable information," the act states: "the term '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." The term "consumer" is defined as "any renter, purchaser, or subscriber of goods or services from a video tape service provider."

The act prohibits VTSPs from disclosing consumers' rental history outside "the ordinary course of business," which VPPA defines as "only debt collection activities, order fulfillment, request processing, and the transfer of ownership." Any such disclosure outside the parameters of the act is deemed an unauthorized disclosure under the law, and may result in statutory penalties at a minimum of $2,500 per aggrieved person. Since modern VTSPs typically hold the PII of thousands, even millions, of consumers, failure to comply with the requirements of VPPA can prove to be quite a costly mistake.

However, VPPA does provide avenues of permissible disclosure to third parties, provided that consumers give informed written consent that:

> (i) is in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer;
>
> (ii) at the election of the consumer—
>
> (I) is given at the time the disclosure is sought; or
>
> (II) is given in advance for a set period of time, not to exceed 2 years or until consent is withdrawn by the consumer, whichever is sooner; and
>
> (iii) the video tape service provider has provided an opportunity, in a clear and conspicuous manner, for the consumer to withdraw on a case-by-case basis or to withdraw from ongoing disclosures, at the consumer's election.

In practice, this means a VTSP seeking to use consumers' PII may do so if consent is clearly and freely given on a separate form. Such consent thus cannot be buried in the VTSP's terms of use or privacy policy. Since this consent is "at the election of the consumer," the VTSP must adhere to an opt-in model of consent. VTSPs must either seek consent on a case-by-case basis, or seek a blanket form of consent for a set period of time. If the latter, that consent must not exceed a period of two years, and the consumer must retain the ability to opt out should they so choose. These restrictions are currently the minimum legal standard that all VTSPs must put into practice to ensure compliance with U.S. law. VPPA's ambiguities are far from settled, but the varied outcomes of prior legal challenges provide significant guidance for those who qualify as VTSPs.

VPPA applied to online video

What viewing habits might reveal about users

One of the earliest examples of a potentially substantial breach of VPPA in the online context is the case of Doe v. Netflix. In September 2006, Netflix sought to improve the accuracy of its film recommendation algorithm and devised a somewhat unconventional means to do so: A contest. Through the Netflix Prize, the company offered whoever could best improve its algorithm a $1 million prize and "gave more than 50,000 Netflix Prize contestants two massive datasets. The first included 100 million movie ratings, along with the date of the rating, a unique ID number for the subscriber, and the movie info."

Although Netflix believed it had sufficiently "anonymized" the users by providing only a unique ID number — thereby excluding this data from the definition of PII under VPPA — two computer science researchers at the University of Texas Austin demonstrated that a collection of movie ratings, when combined with outside information, could be used to reveal users' identities. In a paper published soon after Netflix released the data, professors Narayanan and Shmatikov demonstrated the capacity to re-identify anonymized datasets by combining the Netflix Prize database with reviews published by about fifty people in the Internet Movie Database (IMDb).

The researchers successfully identified two of the users in Netflix's dataset. On December 19, 2009, the aggrieved parties filed a class-action lawsuit against Netflix in the U.S. District Court of Northern California, claiming that Netflix's carelessness in attempting to anonymize their identities constituted a "wrongful disclosure" of PII under VPPA, and demanded "more than $2,500 in damages for each of more than 2 million Netflix customers." The complaint alleges that Netflix should have reasonably known these measures were inadequate, as they launched Netflix Prize a mere two months after AOL infamously released a file of 650,000 anonymized users' search histories, which received extensive media coverage after the users' were successfully re-identified by a journalist.

Additionally, the class-action sought punitive damages to cover those instances where the disclosure threatened particular harm. Using the pseudonym Jane Doe, one of the plaintiffs stated that she was both a mother and a closeted-lesbian, and that many of the films she viewed were gay and lesbian themed. According to the complaint, were the plaintiff's "sexual orientation public knowledge, it would negatively affect her ability to pursue her livelihood and support her family and would hinder her and her children's' ability to live peaceful lives within [her] community."

The Netflix complaint – which does not, of course, carry the weight of a judicial opinion – articulates why something as seemingly benign as what films someone views may nonetheless be quite personal: "A Netflix member's movie data may reveal that member's private information such as sexuality, religious beliefs, or political affiliations. Such data may also reveal a member's personal struggles with issues such as domestic violence, adultery, alcoholism, or substance abuse."

Defining "subscriber" and "PII" under the VPPA

In addition to the question of what practices are sufficient to protect consumers' identities under VPPA, questions have also been raised as to which consumers are protected under the act. The case of In re Hulu Privacy Litigation represents a failed attempt to limit this definition. Hulu, which was accused of sharing users' video preferences in violation of VPPA, attempted to argue that because Hulu was (at the time) a free service, the affected people were not "subscribers" protected by the act, but simply "users." The court rejected this argument, however, and found that the term subscriber does not necessarily involve monetary payment.

Another interesting and largely unsettled question is what constitutes personally identifiable information under VPPA. In a 2015 case in the U.S. District Court for the District of Massachusetts, Yershov v. Gannett Satellite Info. Network, Inc., Gannet, the

publisher of USA Today, was accused of violating VPPA through its USA Today mobile app. Specifically, "every time a user of the App watches a video, the unique identification number of the user's smartphone is provided to a third-party data-analytics company." The court found that the disclosure, combined with the user's Android ID and GPS location, was enough to constitute PII under VPPA, based on the likelihood that such information could be used to identify the user.

However, the court found that Yershov was not properly characterized as a subscriber under VPPA. The court viewed Yershov as a user rather than a subscriber, noting: "Subscriptions involve some or all of the following: payment, registration, commitment, delivery, and/or access to restricted content." As Yershov merely downloaded the App, but did not pay money, register, or make any kind of commitment, the court held that VPPA's protections did not apply to him.

In the 11th Circuit case Ellis v. The Cartoon Network, Inc., a similar charge was brought against Cartoon Network for its mobile app practices. The court likened merely downloading a mobile app to adding a website to one's favorites in a conventional browser and, citing the ruling in Yershov as persuasive, found that Ellis was not a subscriber protected under the act.

However, on appeal from the district court's 12(b)(6) dismissal of Yershov, the 1st Circuit specifically addressed the analogy given in Ellis and rejected it, questioning why Gannett would create a mobile app if it was truly the same as viewing the content in a web browser. The court found that the transaction "whereby Yershov used the mobile device application that Gannett provided to him, which gave Gannett the GPS location of Yershov's mobile device at the time he viewed a video, his device identifier, and the titles of the videos he viewed in return for access to Gannett's video content," effectively made him a subscriber under VPPA.

The future of video privacy regulation

The growing digital economy means that technology and innovation will often grow at a faster pace than the laws that govern them. While industry players will seek to make the most of their products, VPPA remains a potential limitation on any service that provides video content. Based on the currently unsettled climate surrounding VPPA, it is now more important than ever for companies to err on the side of caution, be as specific as possible in disclosures to consumers, and not assume that products are exempt from VPPA.

This need for caution is underscored by the Federal Trade Commission's recent video privacy case, VIZIO, Inc. and VIZIO Inscape Services, LLC. In this case, the FTC asserted for the first time that "sensitive" information — which had previously been limited to financial data, health data, Social Security numbers, children's data, and geolocation data — also includes television and video content viewing data. Although the FTC gave little guidance for finding that entertainment consumption habits are "sensitive" information the misuse of which could cause substantial injury, its Complaint against VIZIO asserted that "[c]onsumers' viewing history is subject to certain statutory privacy protections," citing the Cable Privacy Act. VPPA could potentially serve as an additional public policy basis for adding television and video content viewing to the list of sensitive personal information.