Hashed & Salted | A Privacy and Data Security Update
December 2023

Why Blockbuster Is Relevant Once More: The Return of the VPPA

Thirty-five years ago, Congress enacted the Video Privacy Protection Act (VPPA), 18 U.S.C. § 2710, in response to a video store clerk's leaking a Supreme Court nominee's "dull" videotape viewing habits to a prying reporter.

Although the statute allows a private right of action with high statutory damages, it was rarely litigated until 2007. With the rise of digital media and the internet, the sharing of video-watching habits and preferences became more common. The VPPA, a relic from the heyday of the videotaping era, was relevant once more as consumers sought to apply it to businesses not even contemplated in the 1980s, such as online streaming services, social media platforms, smart home devices and media companies.

Recently, as technology has further evolved and user data tracking has become more commonplace, the VPPA has seen increased litigation activity, particularly in the realm of pixel tracking. This has added an additional layer of complexity for businesses seeking to avoid legal troubles. This article provides a comprehensive overview of the VPPA, including how the statute has been interpreted to apply to digital media. It discusses recent trends in litigation, particularly as they relate to third-party analytics tools like tracking pixels. Finally, it provides practical advice to businesses that collect and share consumers' viewing history and wish to avoid violating the VPPA.

What the VPPA Prohibits

The VPPA prohibits (1) a "video tape service provider" from (2) knowingly disclosing (3) "personally identifiable information" about a (4) "renter[], purchaser[], or subscriber[]" of these services.

After about 2007, litigation under the VPPA essentially focused on how to fit a square peg into a round hole—in other words, how to interpret a statute intended to prevent the Blockbusters of the world from leaking video rental histories of their patrons in light of the proliferation of the internet and social media sharing.

Courts have generally interpreted the statute as follows.

A videotape service provider is any entity that provides prerecorded video content, including those that stream videos through a website, an app, a social media platform or technology with software for internet video content delivery (e.g., smart TVs). A platform that provides only live streams of content is not a videotape service provider under the VPPA.

The disclosure must be knowing—in other words, the business must be aware that its consumers' video history and personally identifiable information (PII) would be combined and shared.

PII must be disclosed. This is information that demonstrates that a certain individual requested to watch the video. Courts have disagreed on what constitutes PII for the purposes of the VPPA.

A consumer—someone who is a renter of, purchaser of or subscriber to a videotape service provider—needs to have their information disclosed.

Attorney Advertising

When Sharing Video History Is Permitted Under the VPPA

Disclosure is permitted in narrow circumstances:

- In the ordinary course of business, which is strictly limited to "debt collection activities, order fulfillment, request processing, and the transfer of ownership."
- To a law enforcement agency in response to a warrant, subpoena or court order.
- Only the name and address of the consumer and (exclusively for the use of marketing goods or services) the subject matter of videos the consumer chooses are provided, and the consumer is given a clear opt-out opportunity.
- Pursuant to a court order in a civic case upon showing a compelling need if the consumer is given reasonable notice and has the opportunity to contest the release of the records.

Disclosure is also permitted if the consumer has given separate informed written consent.

The consent must be voluntary and given (a) at the time the disclosure is sought or (b) in advance for a set period of time (that is no longer than two years) or until consent is withdrawn, whichever is sooner.

The provider must also give the consumer clear and conspicuous opportunities to withdraw consent.

Damages Under the VPPA

The VPPA allows for damages of $2,500 per violation. A plaintiff may instead be awarded actual damages (if said damages are higher than $2,500) by demonstrating that they suffered specific harm as a result of the VPPA violation.

Courts may also award punitive damages in cases where the defendant's VPPA violation was particularly egregious or intentional. If a VPPA violation case is successful, the defendant may be required to pay attorney's fees, litigation costs and other equitable relief the court deems appropriate.

Pixel-Tracking Litigation

Many of the initial VPPA lawsuits of the 21st century were filed against content providers with sites that shared video history information with social media sites.

In the past year, the digital landscape has witnessed a significant uptick in VPPA lawsuits. Almost 100 VPPA actions have been filed against operators of websites in a broad array of industries that offer video clips on their sites. The websites use third-party analytics tools, such as for tracking pixels (e.g., Google Analytics, Doubleclick and Blaze). Plaintiffs are alleging that the use of pixels to collect analytics information violates that VPPA when the pixels collect information about website video views without consent.

While most of these lawsuits have not been fully litigated, courts have been denying motions to dismiss and allowing the cases to proceed to discovery. Defendants have had success with the following defenses:

- **The plaintiffs are not subscribers to the websites.** Courts have disagreed on whether persons who have not provided a monetary payment to watch the video content, the product, can qualify as consumers under the statute. Some courts have found that downloading and using free mobile apps to view freely available content does not qualify the individual as a "subscriber" because there is no ongoing commitment. Others have held that plaintiffs do not need to purchase a subscription or a product to qualify as a consumer under the VPPA.
- **No PII is disclosed.** Generally speaking, some courts have held that information is PII only if an ordinary person (using the information disclosed) can identify the specific watcher of a video. In other words, if a provider disclosed only a randomized ID, it would not qualify as PII under the VPPA. However, if a provider disclosed a randomized ID along with a precise geolocation or a list tying the identifier to a subscriber name, it would qualify as PII. Other courts have disagreed with this holding, stating that any information that can identify an individual is PII, even if the individual can only be identified with information collected from a third party—e.g., smartphone ID, media access control (MAC) address, internet provider (IP) address, geolocation information or social media identification.
- **The defendant is not a videotape service provider.** Recent decisions have confirmed that a business is not a videotape service provider if displaying video is only an ancillary part of its business. However, where that line is drawn may depend on the facts.

What a Business Should Do

1. **Audit Your Websites.** Regularly audit the pixels and other trackers on your website, and have a detailed understanding of the specific pieces of data you are making available to third parties. Understand whether there are opportunities to minimize information sharing that may trigger VPPA risks (e.g., sharing only genre-level information, masking unique identifiers or leveraging clean room technology to gain insights without making video viewing information available to a third party).
2. **Be Transparent.** Clearly communicate your data collection practices, including video viewing history tracking and pixel usage, to users. Provide concise and understandable privacy policies that inform users about what data you collect and why.
3. **Secure Consent.** If you determine that your activities fall within the scope of the VPPA, consider whether and how you can obtain consent (e.g., via a cookie banner). Utilize user-friendly consent mechanisms that make it easy for users to grant or withhold consent.

Related Professional

Daniela Spencer . . . . . dspencer@loeb.com