BCLP. Client Intelligent

Insights

VPPA TRENDS: CONSIDERATIONS FOR LIMITING EXPOSURE

Jul 25, 2023

SUMMARY

In recent months, organizations have been dealing with an emerging wave of lawsuits from an unexpected source: the VPPA. The Video Privacy Protection Act ("VPPA"), originally intended to prevent "wrongful disclosures" of video tape sale and rental data from companies like Blockbuster and Family Video, is being rehabilitated by the plaintiffs' bar to target any video content appearing on websites. Plaintiffs are now alleging that website operators using embedded videos are knowingly disclosing data to third parties through pixels and similar tracking technologies. For organizations caught in the crosshairs, violations of the law may result in statutory damages of $2,500 per violation, as well as attorneys' fees, other monetary relief, and preliminary injunctive relief.[1] Given the large number of users who may access a single website, class actions under the VPPA have resulted in substantial settlements, ranging from $9 million to $92 million.[2]

THE VIDEO PRIVACY PROTECTION ACT

The VPPA prohibits "video tape service providers" from knowingly disclosing "personally identifiable information," which broadly includes any "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider."[3] While the term "video tape service provider" traditionally meant brick-and-mortar stores like Blockbuster and Family Video, the plaintiffs' bar has sought to apply the term to any website operating with embedded videos that shares data with analytics firms and other third parties for marketing purposes.

Recent complaints typically allege that the following actions violate the VPPA:

1. a consumer-facing website contains embedded videos and has implemented certain cookies to support those videos;

2. consumers accessing the website are logged into third party websites — typically social media sites — while viewing videos on the website;

3. an embedded tracking pixel "fires" upon the occurrence of a predetermined event, such as a video view, and transmits data regarding that page, including the title of the video and a unique user ID, to the third party website that tracks the consumer across websites and platforms; and

4. the website operator knowingly disclosed the consumer's video-watching data to the third party tracking providers.

DEFENSE STRATEGIES AND RECENT RULINGS

In general, courts have embraced an expansive view of the scope of the VPPA. More recently, however, signs have emerged that courts are ready to impose limits on its application, interpreting the Act's broad statutory language holistically and with an eye to Congress' original intent in enacting the statute. The new scrutiny has focused on a few key issues, including whether the defendant is a "video tape service provider," whether the plaintiff is a "consumer," and whether "personally identifiable information" has been conveyed to a third party.

VIDEO TAPE SERVICE PROVIDERS

Several federal courts have dismissed VPPA claims where the viewed content was live-streamed, as opposed to pre-recorded.[4] Relatedly, though many courts have accepted at face value that website operators that embed pre-recorded videos on their websites are subject to the VPPA[5], other courts have begun to question the broad application of the law. In a recent decision from a federal court in California, the court dismissed a VPPA claim against a fashion retailer because the defendant's business model was not "significantly tailored" to delivering video content on its website; it was not enough that the company engaged in the peripheral action of providing consumers with access to embedded videos through their retail website.[6]

PERSONALLY IDENTIFIABLE INFORMATION

The VPPA is limited to disclosures of "personally identifiable information." The courts have consistently held that a user ID, typically one that links a user to a social media account, paired with video viewing information is sufficient to constitute personally identifiable information.[7] The First Circuit held that precise GPS coordinates and device ID were sufficient, given the ease with which an individual's identity can be discerned by locating a corresponding home address,[8] while the Ninth Circuit has held that a device serial number and video viewing information was insufficient.[9] A new wave of plaintiffs have alleged that certain social media pixels also transmit personally identifiable information; however, the courts have yet to rule on these allegations.

KNOWING DISCLOSURES OF DATA

Recently, a court dismissed a VPPA claim based on a showing by the defendant, a video streaming service provider, that it did not "knowingly" disclose personally identifiable information to third parties.[10] There, the defendant alleged that there was no evidence that it knew that a tracking pixel was collecting and disclosing personally identifiable information, as defined under the VPPA. Other courts have ruled that merely including certain pixels on a website was sufficient to show a knowing disclosure of personally identifiable information.[11]

CONSUMER

Courts also have dismissed VPPA claims after finding that plaintiffs fall outside of the scope of "consumers." While there is a consensus that a plaintiff need not pay money to be considered a consumer, the circuits have split regarding the degree of commitment a plaintiff must have made to be considered a subscriber. The First Circuit held that downloading a mobile application and providing personal information and GPS coordinates to the defendant was sufficient,[12] while the 11thCircuit held essentially the opposite.[13]

HEIGHTENED PLEADING REQUIREMENTS

Several courts have also found that plaintiffs cannot rely on generally pleading that video watch data automatically includes personally identifiable information; instead, those plaintiffs must plead with sufficient specificity to bring a claim, such as by describing the categories of personally identifiable information subject to disclosure.[14]

As this is a rapidly developing area of law, it is important to review the latest caselaw to understand the latest successful defenses taken by VPPA defendants.

CONSIDERATIONS FOR WEBSITE OPERATORS

VPPA claims continue to proliferate. BCLP assists clients in reviewing their website tracking technologies and their use of embedded videos, and defending organizations that are the subject of VPPA claims. Given the changing nature of VPPA claims and the emergence of key defense trends in response, organizations should be mindful of potential risks and should take several steps to limit potential VPPA class action exposure, such as:

- Limiting the use of pixels and other tracking technologies to pages without video content or configuring pixels and cookies to avoid sharing personally identifiable information with third parties.
- Updating cookie preference centers, or similar mechanisms, to collect separate consent from users prior to disclosing video-watching data.
- Updating the website privacy policy to accurately disclose whether personally identifiable information is disclosed to third parties, and how that personally identifiable information is

used.

FOOTNOTES

[1] 18 USC 2710(a)(3), (b)(1).

[2] *Stark v. Patreon, Inc.*, 2022 WL 7652166 (N.D. Cal. 2022) (holding that "live broadcasts" are not covered by the VPPA); *Louth v. NFL Enterprises LLC*, 2022 WL 4130866 (D.R.I. 2022).

[3] *Yershov v. Gannett Satellite Information Network, Inc.*, 820 F.3d 482 (1st Cir. 2016).

[4] *Cantu v. Tapestry, Inc.,* Case No. 3:22-cv-01974 (S.D. Cal 2023) (Order granting a motion to dismiss).

[5] *Eichenberger v. ESPN, Inc.*, 876 F.3d 979 (9th Cir. 2017).

[6] *See Yershov*, *supra* at n. 5.

[7] *See Eichenberger, supra* at n. 7.

[8] *In re Hulu Privacy Litigation*, 86 F. Supp. 3d 1090 (N.D. Cal. 2015).

[9] *Belozerov v. Gannett Co.,* Case No. 22-10838-NMG (D. Mass. 2022).

[10] *See Yershov*, *supra* at n. 5.

[11] *Ellis v. Cartoon Network, Inc.*, 803 F.3d 1251 (11th Cir. 2015); *Carter v. Scripps Networks, LLC*, Case No. 1:2022-cv-2031 (S.D.N.Y. 2023); *Michael Salazar v. Paramount Global*, Case No. 3:22-cv-00756 (M.D. Tenn. 2023).

[12] *Ambrose v. Boston Globe Media Partners LLC*, 2022 WL 4329373 (D. Mass. 2022).

RELATED PRACTICE AREAS

- Data Privacy & Security

MEET THE TEAM

Amy de La Lama

Boulder

amy.delalama@bclplaw.com
+1 303 417 8535

Christian M. Auty

Chicago

christian.auty@bclplaw.com
+1 312 602 5144

Daniel T. Rockey

San Francisco

daniel.rockey@bclplaw.com
+1 415 268 1986

Gabrielle A. Harwell

Chicago

gabrielle.harwell@bclplaw.com
+1 312 602 5143
