iab.

Video Privacy Protection Act (VPPA)

Litigation Preparation & Defense Toolkit

APRIL 2024

Sponsored by LOEB & LOEB LLP

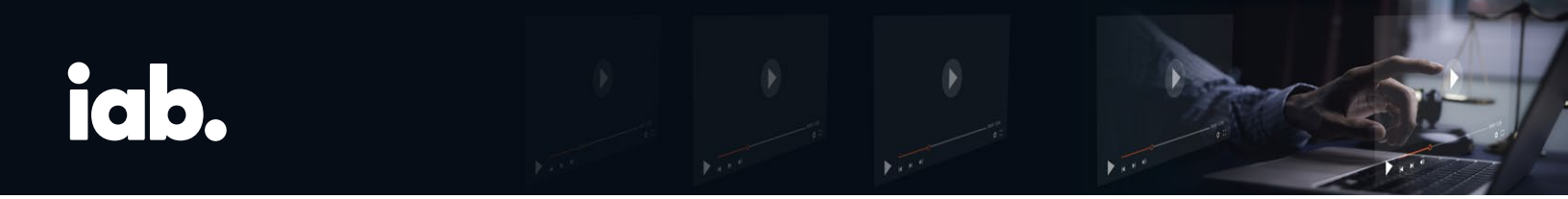
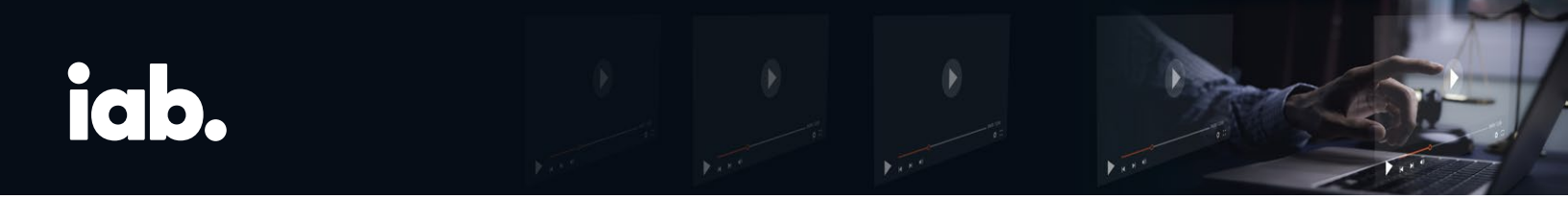


Table of Contents

Disclaimer: The information provided in this white paper is for educational purposes only. It is not intended to serve as and should not be relied upon as legal advice. Companies considering their own specific compliance obligations should consult with qualified legal counsel.

The plaintiffs' bar has commenced a new wave of lawsuits in recent years asserting claims under the VPPA in connection with the alleged use of third-party pixels on websites that offer video content. Pixels are a piece of code embedded on a website that help track users' activities on site, as well as across third-party websites. Pixels generally collect information about user's website interactions (page views, clicks, purchases, etc.). When pixels are embedded on webpages with video content or in video links, they may transmit data that includes the title of the video. The complaints frequently allege that when Meta and other third-party pixels are placed on webpages with video content, they transmit information about the users' video viewing information in violation of the VPPA. The VPPA provides for actual damages, as well as statutory damages of $2,500 per violation.

This toolkit provides an overview of the VPPA, an outline of the key elements of a VPPA claim, a description of the successful and unsuccessful defenses, and proactive next steps to take to avoid a complaint.



I. Overview: What Is the VPPA?

The Video Privacy Protection Act (VPPA)[1] is a federal statute that was enacted in 1988 after Supreme Court nominee Robert Bork's video rental records were published in a newspaper without his consent. The article, titled "The Bork Tapes," drew the ire of Congress, which responded by enacting the VPPA within a year of the article's publication. The law prohibits companies from knowingly disclosing a consumer's personally identifiable information (including their requests or purchases of specific video materials) unless an exception applies.

What are the conditions in which can personal information be disclosed without violating the VPPA?
Personally identifiable information ("PII") can be disclosed to:

- ☐ the consumer;[2]
- ☐ any person with the **informed, written consent** of the consumer;[3]

VPPA consent options:

1) In real time (upon each video view shared), OR

2) In advance, but that consent must be renewed every 2 years. 18 U.S.C. § 2710(b)(2)(B)(ii).

* Note that consent must be separate from a terms of use or privacy policy. See § 2710(b)(2)(B)(i).

- ☐ a **law enforcement** agency, pursuant to a federal or state warrant, a grand jury subpoena, or a court order (subject to specific requirement set forth in the law);[4]
- ☐ any person if the disclosure is limited to the names and addresses of consumers and if:
  - ○ (i) the video tape service provider has provided the consumer with the **opportunity**, in a clear and conspicuous manner, **to prohibit such disclosure**; and

[1] Video Privacy Protection Act of 1988, Pub. L. No. 100-619, 102 Stat. 3195 (1988) (codified at 18 U.S.C. § 2710).

[2] *Id*. § 2710(b)(2)(A).

[3] The statute specifies that the consumer must provide "informed, written consent (including through an electronic means using the Internet)" that is "in a form distinct and separate from any form setting forth other legal or financial obligations of the consumer" and includes an opportunity, provided 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." *See Id*. § 2710(b)(2)(B); *Feldman v. Star Trib. Media Co. LLC*, No. 22-CV-1731 (ECT/TNL), 2023 WL 2388381, at *11 (D. Minn. Mar. 7, 2023) (The federal district court declined to dismiss the VPPA claim based on the Star Tribune's argument that the plaintiff consented to its Privacy Policy referenced in its Terms of Use; the court said "it [was] not obvious that the Star Tribune Privacy Policy addresse[d] a consumer's consent to disclosure of his or her video-viewing history, and it appear[ed] to cover many legal obligations beyond consent to disclose personally identifiable information under the VPPA.").

[4] 18 U.S.C. *Id*. § 2710(b)(2)(C).

- (ii) the disclosure **does not identify the title, description, or subject matter** of any video tapes or other audio visual material; however, the subject matter of such materials may be disclosed if the disclosure is for the exclusive use of marketing goods and services directly to the consumer;[5] or
- any person if the disclosure is incident to the **ordinary course of business** of the video tape service provider;[6] or

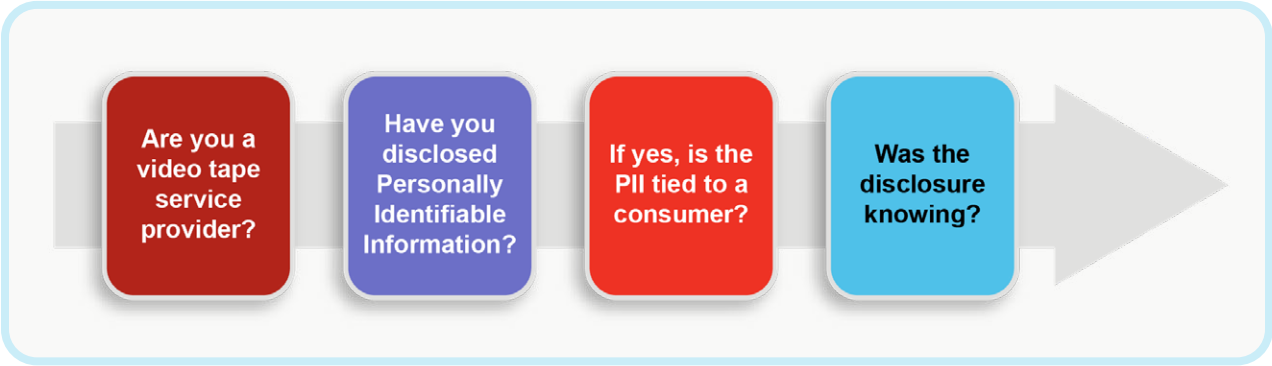
Activities in the ordinary course of business include:

- debt collection activities
- order fulfillment
- request processing
- transfer of ownership

- pursuant to a court order, in a civil proceeding upon a showing of compelling need for the information that cannot be accommodated by any other means (subject to specific requirements set forth in the law).[7]

II. Key Elements To Establish a VPPA Claim

To state a claim under the VPPA, a plaintiff must prove that (1) a "video tape service provider" (2) knowingly disclosed (3) "personally identifiable information" (4) of a "consumer".[8] Claims fail when they cannot establish one of these key elements.



[5] *Id.* § 2710(b)(2)(D).
[6] *Id.* § 2710(b)(2)(E).
[7] *Id.* § 2710(b)(2)(F).
[8] *Id.* § 2710(b)(1).

Are you a Video Tape Service Provider?

Under the VPPA, a video tape service provider is "any person, engaged in the business… of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials." (emphasis added)[9] This definition has been interpreted expansively by the courts to include OTT apps consumers use for streaming, as well as publisher apps with video content.[10]

***Note:** Livestreaming of video content that is not pre-recorded has been held not to give rise to VPPA liability.

PRACTICE POINT:

***Louth v. NFL Enterprises LLC*, 2022 WL 4130866, at *4 (D.R.I. Sept. 12, 2022)**

In *Louth v. NFL Enterprises LLC*, the court granted the motion to dismiss plaintiff's class action VPPA claim with respect to any aspect that is premised upon the consumption of live content. *Id*. at *5.

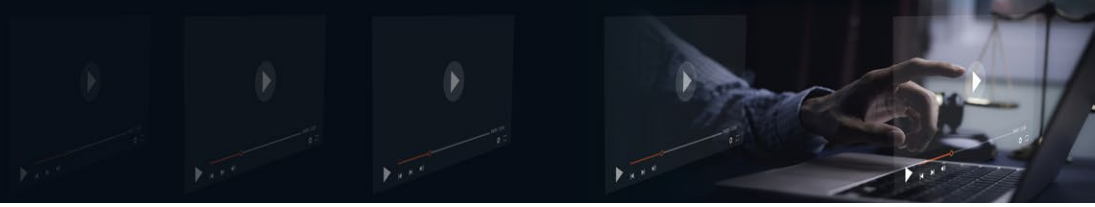
Plaintiff argued that live content should be included as a "similar audio visual materia[l]," within the definition of "video tape service provider." *Id*. at *4.

The court found that plaintiff's interpretation goes too far because the adjective "prerecorded" modifies both "video cassette tapes" *and* "similar audio visual materials." *Id*.

Key Takeaway: Companies do not qualify as a video tape service provider under the VPPA to the extent that they broadcast live videos, which are arguably not similar to pre-recorded videotapes.

[9] *Id*. § 2710(a)(4).

[10] *See, e.g., In re Hulu Privacy Litigation*, No. C 11-0374, 2012 WL 3282960, at *5–*6 (N.D. Cal. Aug. 10, 2012) (holding that Hulu, a video-streaming business, is a "video tape service provider" under VPPA); *Mollett v. Netflix, Inc.*, No. 5:11–CV–01629, 2012 WL 3731542, at *2 (N.D. Cal., Aug. 17, 2012) ("Netflix does not challenge the allegations that it is a 'video tape service provider" and a 'person providing video recording… rental services…'"); *Yershov v. Gannett Satellite Info. Network, Inc.*, 820 F.3d 482, 484 (1st Cir. 2016). "While Gannett[, an international media company offering content in print and through mobile applications like the USA Today Mobile App,] claimed in its motion papers that it is not a "video tape service provider" under the VPPA, it did not challenge the sufficiency of Yershov's pleading as to this element of the claim.").



PRACTICE POINT

***Carroll v. General Mills, Inc.*, 2:23-cv-01746 (C.D. Cal. June 26, 2023)**

In *Carroll v. General Mills, Inc.*, the federal court granted General Mills' motion to dismiss plaintiffs' class action VPPA claim. *Id*.

Plaintiffs alleged that their Facebook IDs, browser identifiers and video-viewing activity were shared with third parties via a pixel installed on General Mills' website. *Id*. at *1. Plaintiffs claimed that General Mills was a video tape service provider subject to the VPPA because it was "in the business" of video delivery through its creation and distribution of online videos to "increase[ ] its brand presence." *Id*. at *3.

The court held that the VPPA "does not cover every company that merely delivers audio visual materials ancillary to its business." *Id*. To sustain a claim under the VPPA, a plaintiff must plead facts demonstrating that a defendant's "particular field of endeavor" is the delivery of audiovisual materials, rather than merely a "peripheral" part of its marketing strategy. *Id*.

In re Facebook Consumer Privacy User Profile Litigation**, 402 F. Supp. 3d 767 (N.D. Cal. 2019)**

In *In re Facebook Consumer Privacy User Profile Litigation*, the court denied Facebook's motion to dismiss plaintiffs' class action VPPA claim. *Id*.

Plaintiffs' alleged that Facebook "regularly delivers video content to users and maintains a cache of videos and visual materials, including from content providers like Netflix, for their delivery to users." *Id*. at 799.

The court found that it was plausible "to conclude from these and related allegations that Facebook engages in the business of delivering audio visual materials, and that its business is significantly tailored to serve that purpose," while also acknowledging the possibility of someone arriving at a different conclusion at summary judgement once the evidence is examined. *Id*.

Key Takeaway: If posting videos online is incidental to a company's core business (e.g. a consumer goods brand that happens to advertise using video content), it is not subject to the VPPA. This is a complete defense to VPPA claims. It is worth noting that determining whether a defendant is "engaged in the business… of rental, sale, or delivery" of video content may be straightforward in cases some cases (e.g., where the defendant directly rents or sells video content or access to such content over the internet), but in other cases it may present close calls (e.g., where the defendant's business could be interpreted as being "significantly tailored" to serve the purposes of delivering video content).

Have you disclosed Personally Identifiable Information (PII)?

Under the VPPA, PII has a narrow definition and is limited to information that in combination identifies:

- ☐ a person (such as a unique pseudonymous ID, email address, or account ID, in combination with other information); and
- ☐ the person's request or receipt of specific video materials or services (such as the titles of videos accessed, requested, or watched).[11]

The courts are split on how the definition of PII applies in the context of modern digital advertising use cases. One court found that IP Address and geolocation, together, are PII, but other courts have been unwilling to find IP address or other device IDs and online identifiers to be PII.[12] The majority of courts have found that PII under the VPPA must be in a form that allows an ordinary person to identify a particular individual as having watched certain videos (as opposed to an IP address or other device IDs and online identifiers, which would require additional information in order to identify the specific individual).[13]

That said, courts have been willing to find that the information collected via Meta's pixel is PII because the Facebook ID can be used by Meta to lookup the identity of the user.[14]

[11] See 18 U.S.C § 2710(a)(3)

[12] *Compare Yershov v. Gannett Satellite Info. Network, Inc.*, 104 F. Supp. 3d 135, 146 (D. Mass. 2015), rev'd, 820 F.3d 482 (1st Cir. 2016). ("the information alleged disclosed to Adobe by Gannett, which consists of an Android ID and a GPS location, constitutes "personally identifiable information" within the meaning of the Video Privacy Protection Act."), *with In re Nickelodeon Consumer Privacy Litig.*, 2014 WL 3012873, at *10 (D.N.J. July 2, 2014) ("[PII is] information which must, without more, itself link an actual person to actual video materials."); *Ellis v. Cartoon Network, Inc.*, 2014 WL 5023535, at *3 (N.D.Ga. Oct. 8, 2014), *aff'd on other grounds*, 803 F.3d 1251 (11th Cir.2015), (PII not disclosed where the third party to whom an Android ID and viewing history were provided had to "collect information from other sources" to identify the plaintiff); *Locklear v. Dow Jones & Co.*, 101 F.Supp.3d 1312, 1318 (N.D.Ga.2015), *abrogated on other grounds*, 803 F.3d 1251 (11th Cir.2015), ("[A] Roku serial number, without more, is not akin to identifying a particular person, and therefore, is not PII." (quotations omitted)); *Eichenberger v. ESPN, Inc.*, C14–463, 2015 WL 7252985 (W.D.Wash. May 7, 2015) (allegation that Adobe "used information gathered from other sources to link plaintiff's Roku device serial number and the record of what videos were watched to plaintiff's identity" failed to state a claim for disclosure of PII under the VPPA).

[13] *Id.*

[14] *See e.g., In re Hulu Priv. Litig.*, No. C 11-03764 LB, 2014 WL 1724344, at *14 (N.D. Cal. Apr. 28, 2014) ("The Facebook User ID is more than a unique, anonymous identifier. It personally identifies a Facebook user. That it is a string of numbers and letters does not alter the conclusion. Code is a language, and languages contain names, and the string is the Facebook user name."); *Robinson v. Disney Online*, 152 F. Supp. 3d 176, 184 (S.D.N.Y. 2015) ("Nor is the information disclosed by Disney equivalent to a Facebook ID.... A Facebook ID… is thus equivalent to a name—it stands in for a specific person, unlike a device identifier.")

PRACTICE POINT

***Feldman v. Star Trib. Media Co. LLC*,** 659 F.Supp.3d 1006 (D. Minn. 2023)

In *Feldman v. Star. Trib. Media Co.*, the court denied the Star Tribune Media Company's motion to dismiss plaintiff's individual VPPA claim. *Id*.

Complaint alleged that the plaintiff subscribed to the Star Tribune in 2011 and regularly watched videos on startribune.com while logged into his Facebook account on the same web browser and device. *Id*. at *2. Whenever he watched a video on the newspaper's website, his viewed-video URLs and his Facebook ID were shared with Facebook through the Facebook Pixel. *Id*.

The court found that the plaintiff adequately pleaded his claim to survive the motion to dismiss, citing the First Circuit's decision that the IP address plus GPS coordinates plus video title met the definition of PII *Id*. at *9. The complaint described how "connecting a Facebook ID to a specific person, a URL to a particular video, and the specific person to the particular video is a reasonably straightforward exercise." *Id*.

Note: In a separate case, the court granted a motion to dismiss when the only information transmitted was the Facebook ID and web page name, but no information about 1) whether there was video content on the page, 2) the title of the video or 3) whether the visitor requested or consumed video content. *Martin v. Meredith Corporation*, 657 F.Supp.3d 277 (S.D.N.Y., Feb. 17, 2023). The court noted that the plaintiff retained the "default settings [of the Facebook Pixel] and has not created any specific events for tracking," thereby limiting its data collection and sharing Facebook. *Id*. at *4.

The distinguishing factor for the Facebook/Meta ID ("Meta ID") appears to be that, unlike other identifiers (e.g. IP address), the Meta ID represents a particular individual for Meta, which allows Meta to identify the person without linking the Meta ID to personal information obtained elsewhere.

Key Takeaway: Transmitting the Meta ID may be sufficient to survive a motion to dismiss when combined with video title information. The key defense to a claim involving the Meta Pixel will lie in whether the pixel is tracking events that would result in video viewing information being transmitted.

If Yes, did you do so "Knowingly"?

The VPPA does not define what constitutes a "knowing" disclosure.[15] Courts are currently grappling with what this means in an online context and have rejected a defendant's motion to dismiss where the defendant knowingly placed third-party pixels on its site (despite arguments that it did not know what information was transferred).[16]

PRACTICE POINT:

Czarnionka v. Epoch Times Ass'n Inc., 2022 U.S. Dist. LEXIS 209067 (S.D.N.Y. Nov. 17, 2022)

In *Czarnionka v. Epoch Times Ass'n Inc.*, the court denied the defendant's motion to dismiss plaintiffs' class action VPPA claim. *Id*.

Complaint alleged that Epoch Times Association ("Epoch"), an international newspaper and media company, programmed Meta's Pixel into its website code knowing Meta would receive video titles and the visitor's Meta ID when a video is watched. *Id*.at *4.

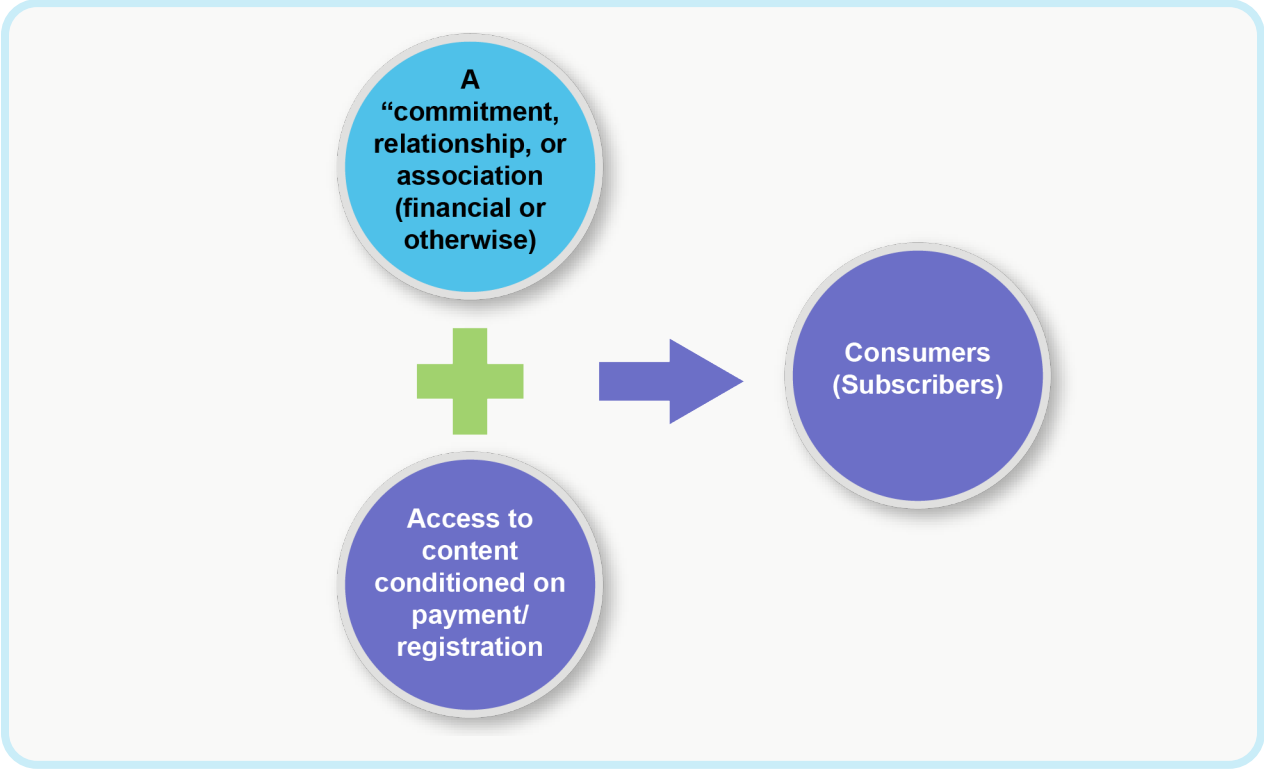
The court found the Plaintiffs' allegation was sufficient to establish that that the company "knowingly" transmitted the information to Meta, even though the complaint did not show that Epoch knew Facebook "might combine a Facebook user's identity (contained in the c_user cookie) with the watch page address [i.e., the URL] to yield 'personally identifiable information' under the VPPA." *Id*. In this case, the court said the "[d]efendant opened a digital door and invited Facebook to enter that door and extract information from within" when it installed the Facebook Pixel. *Id*.at *3.

Key Takeaway: Installing a social media onto a website with videos may be sufficient to establish that you are knowingly transmitting information to Meta. Knowledge of what the social media company might do with the disclosed information to yield PII is unnecessary.

[15] 18 U.S.C *Id*. § 2710(a)(4).

[16] *Czarnionka v. Epoch Times Ass'n, Inc.*, No. 22 CIV. 6348 (AKH), 2022 WL 17069810, at *1 (S.D.N.Y. Nov. 17, 2022), motion to certify appeal denied, No. 22 CIV.6348 (AKH), 2022 WL 17718689 (S.D.N.Y. Dec. 15, 2022); Feldman v. Star Trib. Media Co. LLC, No. 22-CV-1731 (ECT/TNL), 2023 WL 2388381, at *10 (D. Minn. Mar. 7, 2023) ("It follows that a VPPA plaintiff need not allege—to meet the VPPA's "knowingly" element—that the video tape service provider knew that the person to whom personally identifiable information was disclosed would "actually connect" the disclosed information. Allegations plausibly showing that personally identifiable information was consciously disclosed suffice….").

Are your users "Consumers"?



Under the VPPA, a consumer is "any renter, purchaser, or subscriber of goods or services from a video tape service provider."[17] In the cases alleging a violation of the VPPA through the use of a pixel where the consumer does not buy or rent video content, the salient question is whether or not a user of a website or OTT that views video content is a "subscriber" – an undefined term within the VPPA. Courts interpreting the meaning of "subscriber" have held that a subscription does not have to be paid, but it does require a relationship or commitment tied to accessing the video content.[18]

***Note:** Requiring personal information as a condition of watching the video may be sufficient to satisfy the definition.

[17] *Id*. § 2710(a)(1).

[18] *See e.g., Harris,* 2023 WL 2583118, at *3 (plaintiff "registered for a PBS account and provided Defendant her personal information, including her name, address, email, IP address and cookies" and "[i]n return… received periodic newsletters and emails," which the court noted contained "restricted content"); *see also Lebakken v. WebMD, LLC*, 2022 WL 16716151, at *3 (N.D. Ga. Nov. 4, 2022) (plaintiffs provided email address and date of birth to create an online account and in return received periodic newsletters with video content and additionally created a login with WebMD.com).

PRACTICE POINT

Carter v. Scripps Networks, LLC, 670 F. Supp. 3d 90 (S.D.N.Y. 2023)

In *Carter v. Scripps Networks*, the court granted the defendant's motion to dismiss the plaintiff's class action VPPA claim.

Plaintiffs alleged that defendant operated HGTV.com which hosted hundreds of video content and also gave website visitors an option to subscribe to email newsletters which linked to videos on HGTV.com. Plaintiffs alleged they were consumers under the VPPA because they subscribed to defendant's email newsletters. The court granted defendant's motion to dismiss on that ground, reasoning that there was no allegation that "a newsletter subscription was required to access [ ] videos, functioned as a login, or gave newsletter subscribers extra benefits as viewers."

Key Takeaway: Even where a company provides users with the option to register or subscribe in general, a plaintiff must still show that that registration or subscription provided enabled watching video content that would not otherwise be available to the user.

III. Recent VPPA Defenses

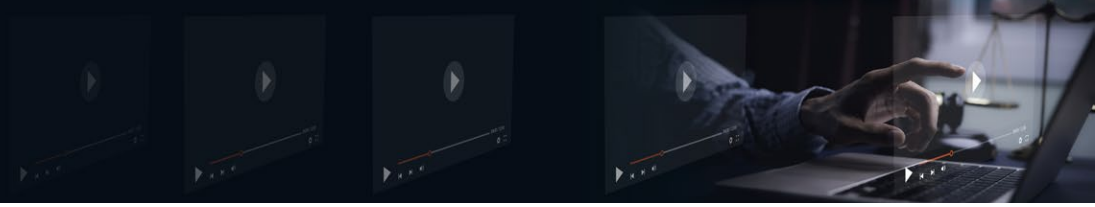
Successful Defenses:

- Defendant is not a **video tape service provider**, because the video content is incidental to the primary business (e.g., marketing video content).[19]
- Plaintiff is not a **subscriber** because viewing video content is not conditioned on paying for the content, registering for an account to access the content, or providing some other consideration (e.g., personal information) in exchange for accessing the content.[20]
- Plaintiff is not a **subscriber** because the subscription was with a third party provider (e.g. a cable provider).[21]
- The information disclosed does not include the title of the video content.[22]

Unsuccessful Defenses:

- The VPPA violates the First Amendment.[23]
- A proprietary social media ID is not **personally identifiable information**.[24]

[19] Carroll v. General Mills, Inc., 2:23-cv-01746 (C.D. Cal. June 26, 2023).
[20] *Gardener v. MeTV*, No. 22 CV 5963, 2023 WL 4365901, at *1 (N.D. Ill. July 6, 2023).
[21] *Perry v. Cable News Network, Inc.*, 854 F.3d 1336, 1342-43 (11th Cir. 2017).
[22] *Martin v. Meredith Corporation*, 2023 WL 2118074 (S.D.N.Y., Feb. 17, 2023).
[23] *Stark v. Patreon, Inc.*, 635 F. Supp. 3d 841 (N.D. Cal. 2022).
[24] *See In re Hulu Priv. Litig.*, No. C 11-03764 LB, 2014 WL 1724344, at *14 (N.D. Cal. Apr. 28, 2014).



- ☐ Defendant didn't **knowingly** share PII and Video Watch History where they placed/ programmed the code that included a social media pixel.[25]
- ☐ A user is not a **subscriber** if the video content is free.[26]
- ☐ The user lacks an injury which an federal court can remedy.[27]

It is also worth noting that the probability of success in VPPA cases may depend on statutory interpretation, as there are a several key terms that are undefined or unclear in light of evolving technology. Certain judges may need help understanding the technical aspects of pixels and similar tracking technologies. Their understanding may be the key factor in how they interpret and apply the grey areas of the law. For example, in *In re Nickelodeon Consumer Privacy Litigation*, the 3rd Circuit held that IP addresses, browser fingerprints, and other persistent identifiers found in advertising cookies did not qualify as personally identifiable information, as the court found that "Congress' purpose in passing the [VPPA] was quite narrow: to prevent disclosures of information that would, with little or no extra effort, permit an ordinary recipient to identify a particular person's video-watching habits," and "to an average person, an IP address or a digital code in a cookie file would likely be of little help in trying to identify an actual person."[28] The court also distinguished the VPPA from the Children's Online Privacy Protection Act (COPPA), explaining that the VPPA, unlike COPPA, does not empower an administrative agency to augment the definition of "personally identifiable information" in light of changing circumstances or new technologies and that the Congress could have amended the VPPA to include persistent identifiers (like COPPA) but chose not to.[29] Notably, the 3rd Circuit said, "[w]e think Congress's decision to retain the 1988 definition of personally identifiable information indicates that the [VPPA] serves different purposes, and protects different constituencies, than other, broader privacy laws."[30] This language is particularly helpful to address arguments for an expansive definition of personal information. As states are increasingly passing comprehensive state privacy legislation with broad definitions of personal information and personal data, plaintiffs' lawyers have already begun to argue that these comprehensive laws should inform the interpretation of personal information under the VPPA.

IV. Proactive Steps to Limit Litigation Exposure

While there is no total shield against a plaintiff's attorney filing a suit against your company, there are proactive steps to limit the risks arising from litigation. These steps can also be used to aid in negotiating a nominal settlement. Additional mitigation measures are available in the Wiretapping Class Action Claims Toolkit.

[25] *Czarnionka v. Epoch Times Ass'n Inc.*, 2022 U.S. Dist. LEXIS 209067 (S.D.N.Y. Nov. 17, 2022)

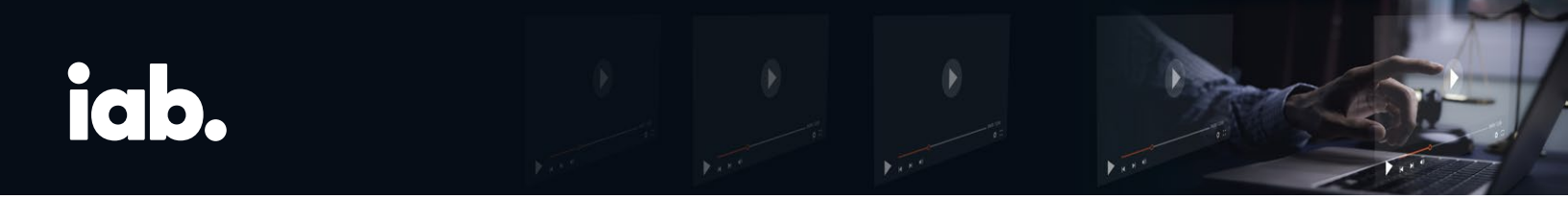
[26] *See Ellis v. Cartoon Network, Inc.*, 803 F.3d 1251, 1256 (11th Cir. 2015) (citation omitted) (noting "[a]lthough most definitions of 'subscribe' or 'subscriber' involve payment of some sort, not all do"); *see also Yershov v. Gannett Satellite Info. Network, Inc.*, 820 F.3d 482, 487 (1st Cir. 2016) ("if the term 'subscriber' required some sort of monetary payment, it would be rendered superfluous by the two terms preceding it").

[27] *See, e.g., Carter v. Scripps Networks, LLC*, 670 F. Supp. 3d 90 (S.D.N.Y. 2023) ("[D]efendants' alleged disclosure of plaintiffs' personal information and viewing activities describes traditionally recognized harm. HGTV's motion to dismiss on standing grounds will therefore be denied.")

[28] *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 282 (3d Cir. 2016).

[29] *Id.*at 287.

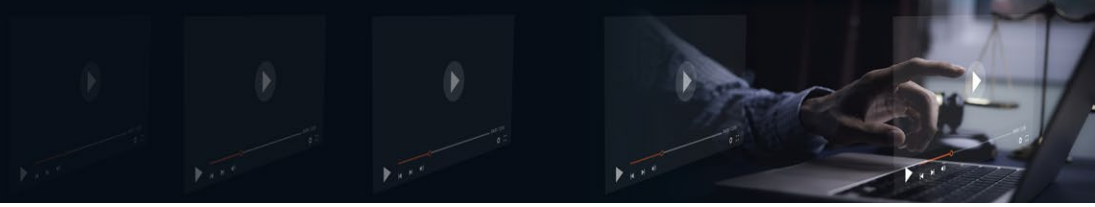
[30] *Id.* at 288.



In sum, companies should assess whether their websites/apps use tracking pixels/cookies/SDKs. If so, they should review and evaluate the implementation of these technologies to determine whether any of the following mitigation measures are possible: (1) removing the tracker from audio-visual materials, (2) obfuscating or removing video title information, (3) taking measures to ensure the information collected is not identifiable, or (4) obtain consent either in real time (upon each video viewed or shared) or in advance (but note that consent expires after 2 years). Implementing a cookie banner to provide notice of tracking practices is also a proposal that appears to be getting more traction as VPPA claims are on the rise.

Policy/Process-Based Steps

- ☐ If the only subscribers you have are subscribers to a product/service that is unrelated to providing access to video content (e.g. newsletter subscribers), avoid posting exclusive video content or access to video content via your newsletters or other similar subscription models (e.g., sign up for texts for exclusive video content).
- ☐ To avoid "subscribers", you can offer users the option to create an account, but you should allow those who do not create an account to access the same content as those with accounts.
- ☐ Do not require consumers to make any commitment to you in a meaningful way to access the video content.
- ☐ Review your privacy policy and disclosures to ensure they accurately and separately reflect any video information sharing practices, including if it is tied to any kind of identifier.
- ☐ Design, deploy and maintain a program to govern the use of pixels, cookies, SDKs and similar technologies on your websites and mobile apps ("Pixel Governance Program"), which aligns your marketing strategy with your privacy obligations. The governance program could include:
  - ☐ Vendor Assessments.
    - ○ Assess the data collection, use, and sharing practices of any SDKs implemented in your mobile app, in addition to documenting the SDK's use case and other privacy and security practice.
    - ○ Design and maintain due diligence process for any vendors that are directly engaged to provide services that involve placing online trackers on your website.
  - ☐ Contractual Protections
    - ○ Determine whether data access and use agreements are in place with authorized online trackers, and that such agreements set forth the data the authorized online trackers may collect, the purpose for the collection, the use of the data, and whether it can be shared, sold, combined, or otherwise matched with other data. The agreements should include audit rights and a process for deletion/removal.
    - ○ If you do not have a direct relationship with the companies providing online trackers, require that the party engaging these companies (e.g. advertisers, if you are a publisher) have these terms in place or require adherence to an industry agreement (e.g. the IAB's Multi-State Privacy Agreement (MSPA)).



- ☐ Tracker Inventory
  - Inventory and categorize identified online trackers by functionality.
  - Design and deploy an ongoing process that documents when and under what conditions online trackers are allowed on your website and the steps entailed to facilitate those trackers placed on your website. Address the conditions for the removal of approved online tracking technologies and documentation reflecting adherence to this process.
  - If this is not currently centralized, consider having one person in each relevant department tasked with monitoring this process on a per department/group basis.
- ☐ Tracker Monitoring
  - Establish a process to confirm that only authorized trackers are running on your platforms.
  - Determine whether an online tracker is not authorized if there is no justification for retaining the tracker.
  - Sunset online trackers once their use case/campaign has ended.
  - Implement a program to facilitate website scanning and monitoring for online tracking on a regular and consistent basis.
- ☐ Implement Consent Management
  - Implement consent management technologies that are properly configured to align with your consent obligations (including opt-out as may be required by applicable law) and overall consent strategy, including use of a tag manager.
  - Document data collected by online tracking technologies on your website
- ☐ Training
  - Implement training to all relevant teams so that they understand pixel-related issues.

Technology-Based Steps

- ☐ Program the social media pixels to limit the data shared.

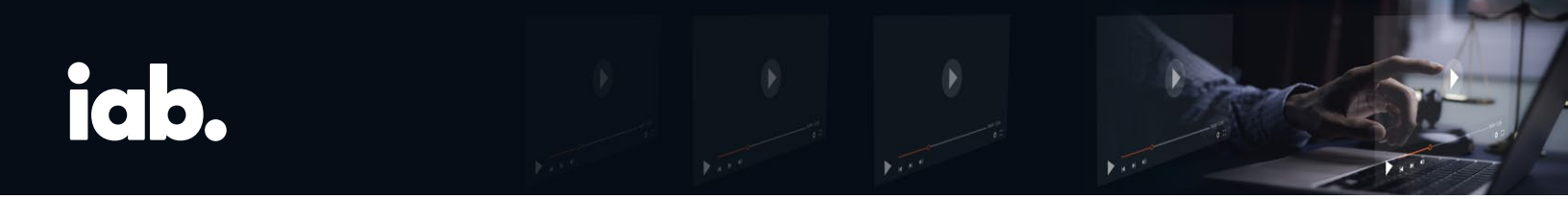
DO NOT SHARE	OK TO SHARE

• Video:
  ○ Title
  ○ Description
  ○ Subject matter of the video
• ACR Data
	• Genre
	• Analytics unrelated to content (e.g., time spent on the page)

- ☐ Use a one-way hash to mask the video title and other relevant video-related data.

Obtain consent. If you are a video tape service provider, you have subscribers, and you want/need to share video titles via pixels, you will need to get consent.

- ☐ Consent must be distinct and separate (e.g., a separate checkbox from the privacy policy and terms)
- ☐ If you obtain advance consent, create a mechanism to track the time and data contained is obtained and automate prompting the consumer for connect every two years.
- ☐ Maintain records of the consent mechanism.



Appendix A– Technologies at Issue in VPPA Cases

1. What is a cookie?

A cookie is a piece of code that stores information on a browser. A first party cookie is a piece of code placed on a browser by that website's web server. Third party cookies are placed by a website from a domain other than the one the user is visiting. For example, if your website has a social media like button, that button will set a cookie that can be read by that social media company. Likewise, the ad server used to serve ads on a website will set cookies that assign a unique ID to a website visitor, which allows the ad server to record relevant touchpoints for that user.

2. What are pixels and why do companies use them?

Pixels are a piece of code embedded on a website that helps track user activities on site, as well as across third-party websites. They are often provided by third parties. While pixels are like cookies (both are tracking technologies that collect data used for analytics, targeted advertising, and improving user experience), there are some key differences:

- Storage: Pixels send the information they collect directly to the third party's servers, whereas cookies store information in a user's browser so the web server can read it again later.
- Tracking: Pixels follow users across devices, while cookies are browser/device specific.
- User control: Consumers can clear or block cookies via their browser settings. Pixels cannot be similarly cleared and are harder for consumers to disable.
- Visibility: Pixels are transparent, single image pixel, that is embedded in the HTML code of an ad or website. It is harder to "see" a pixel when it is on the page.

3. What type(s) of information do pixels collect and who places them?

Pixels generally collect information about user's website or app interactions. This could include (but is not limited to) identifying data (e.g., name, email or hashed email, account or customer ID, device ID), header information (e.g., web page URL, IP address, device/browser type), and events data (e.g., video views and/or URL of video content, items placed in shopping cart, items purchased, information entered on forms, searches performed, information retrieved).

Pixels may be placed by a company directly or by vendors, advertisers or other AdTech partners.

4. Does it matter where the pixel is placed (on website or ad creative)?

No. The important thing to understand is whether the data being disclosed by digital property through the third-party pixel to the pixel provider contains the URL/event title or any other information that could be deemed as PII under the VPPA.

5. Are there other tracking tools that raise VPPA concerns?

In the mobile app environment, companies are more likely to leverage SDKs (software development kits). SDKs are a package of tools that help an app function. SDKs allow companies to build and scale apps quickly without having to build the functionality internally. SDKs can facilitate the collection and disclosure of personal data, depending on how they are configured.