Legal Backgrounder

WASHINGTON LEGAL FOUNDATION
Keeping Free Enterprise Free

Vol. 41 No. 5 April 27, 2026

Video Privacy Law Litigation: The Best Reading of "Personally Identifiable Information"

by Molly Jennings and Anneke Dunbar-Gronke

These days, most video content is consumed through some kind of online platform. Video stores are few and far between—and those that do exist rarely carry video tapes—but certain laws previously passed to regulate them remain active and are being applied to new video technologies. Congress passed the Video Privacy Protection Act (VPPA) in 1988 to prevent "video tape service provider[s]" from sharing personally identifiable information about customer video rental histories. *See* S. Rep. 100-599, at 8 (1988). But plaintiffs and some courts are stretching this law to apply to the new, evolving, and technologically distinct video-viewing landscape of the 21st century. At present, courts are split on whether certain tools used by websites to track and relay user activity to third parties violate the VPPA when that relay includes a user's viewing history. As discussed below, the VPPA should not apply to such tools.

The Video Privacy Protection Act (VPPA) was enacted in 1988 to "extend privacy protection to records that contain information about individuals." S. Rep. 100-599, at 1. The law bars "video tape service provider[s]" from "knowingly disclos[ing]" "personally identifiable information" that concerns "any consumer of such provider" without consent. 18 U.S.C. § 2710(b). The statute defines "personally identifiable information" as "information which identifies a person as having requested or obtained specific video materials or services from a video tape service provider." *Id.* § 2710(a)(3). It also permits consumers to "sue persons who disclose information about their video-watching habits." *In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 278 (3d Cir. 2016). Aggrieved consumers may obtain a minimum amount of $2,500 per violation, and possibly punitive damages, attorneys' fees, and litigation costs. 18 U.S.C. § 2710(c).

Congress enacted the VPPA following the disclosure and publication of 146 films during Judge Robert H. Bork's Supreme Court nomination hearings that he and his family had rented from a video store. S. Rep. 100-599, at 5. As originally conceived, the statute's purpose was to "define the right of privacy by prohibiting unauthorized disclosure of personal information held by video tape providers" and "preserve personal privacy with respect to the rental, purchase, or delivery of video tapes or similar audio visual materials." *Id.* at 6, 9.

Since 1988, however, video technology and the methods by which we access videos have changed drastically. The public has gone from renting video tapes from brick-and-mortar stores to streaming videos online directly from specific websites and through online film and television

---

Molly Jennings is a Partner and **Anneke Dunbar-Gronke** is a Counsel with WilmerHale in the firm's Washington, D.C. office.

apps. And disclosure of video viewing history most commonly happens today via pixel, which is an invisible string of code that can be installed onto a website or an app and can be used to track a visitor's activity. Some companies provide pixels to website operators to assist in tracking user activity for a variety of purposes, including improving user experience and ad targeting. As part of this set up, the activity tracked by these pixels is typically relayed to the company that provides the pixel.

These changes have created opportunities for application of the VPPA in novel contexts. Today, VPPA complaints typically allege that a company's use of software—like a pixel—that gathers and relays users' interactions with a website violates the law. Even companies that do not provide video tapes, like movie theaters, newspapers, and sports websites, are seeing a significant uptick in lawsuits based on their use of web tracking technology now common across the internet.

To its credit, Congress amended the VPPA in 2013, recognizing that the internet had "revolutionized the way that American consumers rent and watch movies and television programs." S. Rep. No. 112-258, at 2 (2012). Through the 2013 amendments, Congress intended for "consumers to [be able] to share information about their video preferences through social media sites on an ongoing basis" without the requiring consent for each disclosure as the old version of the VPPA would have required. *Id.* at 2-3. But website pixel technology as we know it today was still relatively new in 2013, and the 2013 amendments did not resolve the open questions now being tested through litigation seeking to apply the VPPA to website operators' use of pixels.

One line of recent cases has considered whether the definition of "consumer," which the Act defines as "any renter, purchaser, or subscriber of goods or services from a video tape service provider," extends to consumers who have purchased "goods or services" that are not audiovisual in nature. *See, e.g. Pileggi v. Washington Newspaper Publ'g,* 146 F.4th 1219 (D.C. Cir. 2025)*; Gardner v. Me-TV Nat'l Ltd. P'ship*, 132 F.4th 1022 (7th Cir. 2025)*; Salazar v. Nat'l Basketball Ass'n,* 118 F.4th 533 (2d Cir. 2024). Another has explored how to define "personally identifiable information" covered by the Act, and specifically whether the information typically relayed by web tracking software, such as IP addresses, device type, timestamps, and user actions, qualifies. *See, e.g.*, *Solomon v. Flipps Media Inc.*, 136 F.4th 41 (2d Cir. 2025); *Eichenberger v. ESPN, Inc.*, 876 F.3d 979 (9th Cir. 2017); *Yershov v. Gannett Satellite Info. Network*, 820 F.3d 482 (1st Cir. 2016); *In re Nickelodeon*, 827 F.3d at 262.

The Supreme Court granted certiorari to review a consumer definition case, *Salazar v. Paramount Global*, for the October Term 2026. No. 25-459 (U.S. Jan. 26, 2026). There, the plaintiff appeals a Sixth Circuit ruling that refused to revive his proposed class action accusing Paramount of illegally sharing newsletter subscribers' personal information. On review, the Court will decide whether the phrase "goods or services from a video tape service provider," as used in the VPPA's definition of "consumer," refers to all goods and services offered by a video tape service or only its audiovisual offerings. Cert. Pet., *Salazar v. Paramount Glob.*, No. 25-459 (U.S. Oct. 10, 2025).

The Court's decision in *Salazar v. Paramount Global* will not, however, address the other core definitional question related to the VPPA that has divided the Courts of Appeals: what qualifies as "personally identifiable information." Indeed, the Supreme Court rejected a recent petition for certiorari presenting this question in *Hughes v. NFL*, No. 25-868 (U.S. Mar. 9, 2026).

In the absence of guidance from the Supreme Court on what counts as "personally identifiable information," the lower courts have been left to navigate a deepening circuit split. The Second, Third, and Ninth Circuits agree that "personally identifiable information" covered by the VPPA excludes

information that an ordinary person would not be able to use to identify a viewer. The Third Circuit has held that the VPPA applies "only to the kind of information that would readily permit an ordinary person to identify a specific individual's video-watching behavior," *In re Nickelodeon*, 827 F.3d at 267, and the Ninth Circuit has followed suit, *see Eichenberger*, 876 F.3d at 984-985 (concluding "'personally identifiable information' covers some information that *can be used* to identify an individual," but that the Third Circuit's "ordinary person" standard is correct). The Second Circuit has also specifically concluded that this "ordinary person" standard excludes information transmitted by pixels from the definition of "personally identifiable information." In *Hughes v. NFL*, 2025 WL 1720295 (2d Cir. Jun. 20, 2025), the plaintiff—an NFL website user—sued the NFL under the VPPA for using a pixel on its website and app. The question on appeal was whether Hughes could plead a viable VPPA claim in light of Second Circuit precedent holding that the statutory definition of personally identifiable information "encompasses information that would allow an ordinary person to identify a consumer's video-watching habits, but not information that only a sophisticated technology company could use to do so." *Solomon v. Flipps Media*, 136 F.4th 41 (2d Cir. 2025); *see Hughes*, 2025 WL 1720295, at *2. Relying on *Solomon*, the *Hughes* panel affirmed the dismissal of plaintiff's case, holding that the code transmitted via the relevant pixel did not qualify as personally identifiable information because it was "not plausible that an ordinary person" would see that code "and conclude the phrase" was connected to a unique identifier. *Hughes*, 2025 WL 1720295, at *3.

The First Circuit, on the other hand, has interpreted "personally identifiable information" capaciously, to encompass not just information that identifies an individual directly, but also information that would "enable most people to identify" an individual. *Yershov*, 820 F.3d at 486. In contrast with the approach adopted by the Second, Third, and Ninth Circuits, the *Yershov* definition of "personally identifiable information" extends to unique user and device identifiers, GPS coordinates, and any information for which "the linkage" between the information and an individual "is both firm and readily foreseeable." *Id.*

The Second, Third, and Ninth Circuits' approach is correct for several reasons.

First, a narrow construction of "personally identifiable information" under the VPPA is appropriate for today's technology landscape. In a world where online video delivery is virtually inseparable from routine internet operation, interpreting the VPPA to proscribe transmission of code and digital identifiers "decipherable only by a technologically sophisticated third party" could bring scores of popular media and social media sites to a grinding halt. *Solomon*, 136 F.4th at 52. Indeed, if the disclosure of information that *might* result in a third party combining it with other datasets to identify someone specifically, then any standard analytics or fraud-prevention transmission could arguably become a VPPA violation. The Second, Third, and Ninth Circuits' ordinary-person limitation prevents that collapse by distinguishing between (1) data that itself conveys "this specific person watched *this* video," which is exactly the kind of event the VPPA was intended to target, and (2) data that could become identifying only through downstream, expert-level correlation.

Second, the "ordinary person standard" both conforms to the text and purpose of the VPPA and makes intuitive sense. Congress did not define "personally identifiable information" as any data that *could* be linked to a person with enough auxiliary information; it defined the term as "information which identifies a person as having requested or obtained specific video materials or services." 18 U.S.C. § 2710(a)(3). Read naturally, "identifies" denotes information that, on its face, points to a particular person as the viewer of particular content. That ordinary-language limit is especially important in a statute that imposes liability for "knowingly disclos[ing]" covered information, *id.*

§ 2710(b): providers can only "knowingly" disclose what is reasonably recognizable as identifying, not what becomes identifying only after a sophisticated recipient performs multi-step matching analysis to ascertain a viewer's identity. That's not to say that the definition should be read to exclude all information that does not "explicitly name[] a person," *Yershov*, 820 F.3d at 486; it simply means that the definition is limited to information that an ordinary person could use to "identif[y] a person as having requested or obtained specific video materials."

The purpose and structure of the law support this definition. The VPPA was specifically intended to "extend privacy protection to records that contain information *about* individuals." S. Rep. 100-599, at 2 (emphasis added). Concerned with potential privacy intrusions "directly affect[ing] the ability of people to express their opinions," "join in association with others," and enjoy the freedom and independence that the Constitution was established to safeguard," the law's drafters were concerned with ensuring people could "read books and watch films without the whole world knowing." *Id.* at 7. In fact, Congress specifically considered the fact that "[r]ecords of our reading and viewing histories" were being "maintained by libraries, and cable television and video companies," *id.* at 8, but considered only the possibility of those records being disclosed in a format that would "link[]" a person to "particular materials or services," *id.* at 7, not as a collection of "static digital identifiers" that could, only "in theory, be combined with other information to identify a person," *In re Nickelodeon*, 827 F.3d at 283. Moreover, Congress provided several exceptions to the disclosure prohibition that make clear that the VPPA was not intended to prevent "ordinary course" business operations, 18 U.S.C. § 2710(b)(2)(E), or the disclosure of "names and addresses of consumers" along with the "subject matter of [consumed] materials" if for the purpose of "marketing goods and services directly to the consumer," so long as the consumer has had an opportunity to object, *id.* § 2710(b)(2)(D).

Finally, the "ordinary person standard" better informs video service providers of their actual obligations under the VPPA. The ordinary person standard supplies ex ante guidance by offering an objective rule—do not share information that would allow an ordinary person to identify a consumer's video-watching habits. By contrast, an expansive approach would make obligations turn on facts outside the provider's reasonable knowledge, such as the recipient's reidentification capabilities. And since most online video service providers—like most websites—integrate any number of third-party services for security, content delivery, debugging, or to promote user experience that may transmit technical strings, the First Circuit's approach would effectively hold providers liable for standard website integrations that make fast and effective web browsing possible.

Further, the First Circuit interprets the statutory language to be effectively unbounded. Noting that Congress used the word "includes" in its definition of "personally identifiable information," the *Yershov* panel concluded that "the proffered definition falls short of capturing the whole meaning," which includes "[m]any types of information other than a name [that] can easily identify a person." 820 F.3d at 486. But such an overbroad interpretation could mean that any of the myriad data fields that comprise an individual's digital footprint—and that are necessary for the kind of seamless user experience most internet users expect in today's age—would give rise to VPPA liability if any video content is embedded on a website. It could also lead to the perverse results of websites adding consent pop-ups for every webpage with a video, removing the very video content that website users want to see, or, most extraordinarily, enormous statutory damages for using commonplace pixels—at the rate of $2,500 per violation, every visitor who watches a video on a given website could run up the violation multiplier exponentially.

