No. 25-459

IN THE
Supreme Court of the United States

MICHAEL SALAZAR, INDIVIDUALLY AND ON BEHALF OF ALL OTHERS SIMILARLY SITUATED,

Petitioner,

v.

PARAMOUNT GLOBAL, DBA 247SPORTS,

Respondent.

On Writ of Certiorari to the U.S. Court of Appeals for the Sixth Circuit

BRIEF OF *AMICI CURIAE* ELECTRONIC PRIVACY INFORMATION CENTER (EPIC) AND EIGHTEEN TECHNICAL EXPERTS AND LEGAL SCHOLARS IN SUPPORT OF PETITIONER

ALAN BUTLER
Counsel of Record
JOHN DAVISSON
THOMAS MCBRIEN
SARA GEOGHEGAN
HAYDEN DAVIS

ELECTRONIC PRIVACY INFORMATION CENTER (EPIC)
1519 New Hampshire Avenue NW
Washington, DC 20036
(202) 483-1140
butler@epic.org

April 24, 2026

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF THE *AMICI CURIAE*

This brief is submitted on behalf of *amici curiae* EPIC and a group of technical experts and legal scholars whose work concerns issues of online privacy.

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1]

EPIC works to preserve the fundamental right to privacy for all people in the digital age. We conduct research on privacy risks and provide technical expertise on privacy laws and regulations to policymakers, reporters, and to the public.

The technical experts and legal scholars who join this brief include leaders in the field of data privacy whose works are widely cited and relied upon in applying and understanding privacy regulations and data protection systems. The brief does not reflect the views of their institutions. Signatories list their affiliations for identification purposes only.

Anita L. Allen
Henry R. Silverman Professor of Law Emeritus
Professor of Philosophy Emeritus
University of Pennsylvania Carey Law School

David Brody
Privacy and Civil Rights Expert

---

[1]In accordance with Rule 37.6, the undersigned states that no monetary contributions were made for the preparation or submission of this brief, and this brief was not authored, in whole or in part, by counsel for a party.

Ryan Calo
Virginia and Prentice Bloedel Professor
University of Washington

Danielle K. Citron
Jefferson Scholars Foundation Schenck Distinguished Professor of Law
Martha Lubin Karsh and Bruce A. Karsh Bicentennial Professor of Law
Director, LawTech Center
University of Virginia School of Law

Veena Dubal
Professor of Law
University of California, Irvine School of Law

Serge Engleman
Director, Usable Security and Privacy
International Computer Science Institute

Michele Goodwin
Linda D. & Timothy J. O'Neill Professor of Constitutional Law and Global Health Policy
Georgetown Law

Woodrow Hartzog
Andrew R. Randall Professor of Law
Boston University School of Law

Jerry Kang
Ralph and Shirley Shapiro Distinguished Professor of Law
UCLA School of Law

Susan Landau
Professor, Computer Science
Senior Fellow, The Fletcher School
Director, Cybersecurity Center, Computer Science
Tufts University

Anna Lysyanskaya
James A. and Julie N. Brown Professor of Computer Science
Brown University

Neil Richards
Koch Distinguished Professor in Law
Co-Director, Cordell Institute
WashU Law

Pamela Samuelson
Richard M. Sherman Distinguished Professor of Law
Berkeley Law School

Andrew Selbst
Professor of Law
UCLA School of Law

Bruce Schneier,
Fellow and Lecturer
Harvard Kennedy School

Daniel Solove
Bernard Professor of Intellectual Property and Technology Law
Faculty Co-Director, GW Center for Law & Technology

Faculty Director, Privacy & Technology Law Program
George Washington University Law School

Katherine J. Strandburg
Pauline Newman Professor of Law
Faculty Director, Information Law Institute
New York University

Ari Ezra Waldman
Professor of Law
Faculty Director, Center for Technology & Justice
University of California, Irvine School of Law

SUMMARY OF THE ARGUMENT

This case is about a media company transferring information about people's video-viewing habits to one of the largest advertising companies in the world without their consent. Congress recognized this type of disclosure for what it was: an unacceptable invasion of privacy. Yet the lower court in this case held that the Video Privacy Protection Act ("VPPA") did not protect Mr. Salazar, even though he had a subscription to Paramount's services offered by 247Sports, because he was not the right type of "consumer" to fall within the Act's ambit. The lower court's interpretation is contrary to the plain text of the statute and goes against Congress's clear intent to limit disclosure of personal information about video-viewing history.

Congress recognized the uniquely sensitive nature of video-viewing records. In enacting the VPPA, it issued a strong and bipartisan condemnation of the invasion of Judge Robert Bork's privacy through the disclosure of his video tape rental records. And it created a structure to protect individuals from those types of invasions in the future. This law has stood the test of time even as the media landscape has evolved and new technologies have made it easier than ever to access video content. Congress reaffirmed the importance of this law when it passed amendments on a bipartisan basis in 2013.

All signs in the legislative text and history indicate that this law creates strong protections for video-viewing data held by businesses offering video services. Nothing in the legislative history indicates an intent by Congress to distinguish between different categories of consumers in the video-viewing marketplace. Indeed, the Act's definitions use broad and

flexible language that has avoided the interpretive pitfalls that can befuddle regulations of specific technologies or business categories. The key elements that trigger coverage under the VPPA are: (1) a business's provision of video services, (2) a commercial relationship between that business and a consumer, and (3) the improper disclosure of personally identifiable information about that consumer's video-viewing activities. The plain text of the Act does not demand more.

Paramount has tried to support its atextual "consumer" test in this case by arguing that the VPPA was not meant to cover disclosures by video providers to third parties via web tracking technologies, and by implying that a plain meaning interpretation of the statute would "transmogrify it into a prohibition against targeted advertising on the Internet." Br. Opp. Cert. 1. But there is nothing about the Internet, or about targeted advertising, that requires any company to disclose personally identifiable information about a consumer's video-viewing activities to a third party. The fact that Meta's Pixel system causes websites to disclose this private information to Meta is not a legal defense. Unless a video provider obtains informed, written consent from a consumer under 18 U.S.C. § 2710(b)(2)(B), it should not be using any tracking system that discloses individualized user data about access to videos. Paramount, or any other video provider, is not under any obligation to use these systems, and it can adopt more privacy protective techniques to integrate with its advertising and other vendors.

Anyone is free to advocate for a weaker video privacy law. That change would be the ill-advised and politically unpopular. But Congress—not this Court—is the proper venue for such arguments.

ARGUMENT

The Video Privacy Protection Act, 18 U.S.C. § 2710, is even more important today than it was when Congress enacted the law in 1988. Video streaming services have become ubiquitous, vastly expanding the amount and types of personal data that can be collected about video viewers. Tracking and profiling that was merely theoretical in the 1980s is now possible with data analysis tools that anyone with a computer can access. This digital transformation has made strong privacy protections more necessary than ever.

Regulations about data practices and emerging technologies can seem quite complicated, but the VPPA is refreshingly simple. Video service providers are required to protect the privacy of their customers' personal information. And consumers can choose to give express permission to a provider if they want their data to be disclosed. Congress amended the statute in 2013 to ensure that the consent exception would function in the online ecosystem. But they left in place, and reaffirmed the importance of, the statute's core privacy protections for all consumers who access video content.

The Court should reverse the judgment of the Sixth Circuit below because the term "consumer" in the Act has a clear and broad meaning that encompasses any individual who has a commercial relationship with a video tape service provider. This interpretation is consistent with the statute's purpose, as we explain in Section I. And the Act's restrictions on disclosure of personal information do not pose an insurmountable barrier to Paramount or any other business, as we explain in Section II.

I. The VPPA protects the right to view videos privately for all consumers who request specific video materials.

The purpose of the VPPA is to keep sensitive information about individuals' personal video-viewing history private. Congress wanted to protect Americans' freedom to watch the videos they choose without fear that this information will be made public or shared with others. The statute's broad definition of the term "consumer" reflects this. When an individual (1) rents, purchases, or subscribes to any product or service, (2) offered by a video tape service provider ("VTSP"), and (3) the provider collects information about specific video materials the individual requested or obtained from the provider, the Act prevents that provider from disclosing the customer's personal information to third-parties without express, informed consent. The lower court's atextual narrowing of the "consumer" definition to provide these protections to a more limited subset of users undermines the law's purpose and would create a nonsensical, unworkable distinction between covered and non-covered customers.

A. Congress recognized that video-viewing records are uniquely sensitive.

Congress's clear and explicit purpose in enacting the VPPA was to limit disclosure of information about people's video-viewing habits. The history of the development and enactment of the law shows Congress recognized that such information is highly sensitive and should be kept strictly private between the customer and the provider.

In 1987, President Reagan nominated Judge Robert Bork to the U.S. Supreme Court, sparking a high-profile standoff in the Senate. The prominent

judge was known in his jurisprudence for opposing the concept of a general constitutional right to privacy under *Griswold*, and a local reporter asked the clerk at his neighborhood video rental shop to give him a copy of Bork's rental list so that he could write a story about the Judge's personality—while making a tongue-in-cheek point about privacy. *See* Michael Dolan, *Borking Around*, New Republic (Dec. 20, 2012).[2]

While the contents of "The Bork Tapes" were relatively innocuous, their disclosure sparked bipartisan outrage in Congress, *see* S. Rep. No. 100-599, at 5 (1988) (quoting Hearings on Nomination of Robert H. Bork, 100th Cong., 1st Sess. 1372 (Sept. 28, 1987)). One lawmaker noted that the disclosure of these records "seem[ed] more real than anything [he had] know[n] about the right to privacy after practicing law for 18 years." *Id.* The VPPA was signed into law on November 5, 1988, barely thirteen months after the article was published in the City Paper, serving to ensure that this information was adequately protected.

Yet the Act's purpose was not constrained to the disclosure in the Bork case. The Senate Report cites other incidents of unauthorized disclosures of video-viewing information, including one case where "the attorney for a woman in a child custody proceeding [obtained] the records of every film rented by her husband in an effort to show that, based on his viewing habits, he was an unfit father." *Id.* at 6. Indeed, the legislative history shows that the VPPA was not tailored to any one type of unauthorized disclosure, but rather to protect the privacy of video-viewing information held by providers more broadly. *See, e.g.*, *id.* (describing the

---

[2] https://newrepublic.com/article/111331/robert-bork-dead-video-rentalrecords-story-sparked-privacy-laws.

VPPA as "attempt[ing] to give meaning to, and thus enhance, the concept of privacy for individuals in their daily lives"). This was not just a law about judges, or about physical video stores, or about purchase logs. Rather, the statute was written broadly and flexibly to apply robust privacy protections to the broader "social practice" of video-watching at home, enabled by this new burgeoning industry. Neil Richards, *Why Privacy Matters* 58 (2021).

Congress was clear that it considered video-viewing records to be deeply personal and unusually sensitive. That is what animated their efforts to give this specific category of personal information special protection. As Senator Paul Simon, one of the Act's sponsors quoted in the Senate Report, explained, "These records are a window into our loves, likes, and dislikes." S. Rep. No. 100-599, at 6–7 (1988) (quoting 134 Cong. Rec. S5401 (May 10, 1988)). During hearings, lawmakers described the media covered by the VPPA as "the intellectual vitamins that fuel the growth of individual thought," and emphasized how important it is that Americans be able to engage in the "intimate process" of such growth in private, "protected from the disruptive intrusion of a roving eye." S. Rep. No. 100-599, at 7 (quoting Rep. McCandless).

In essence, with the VPPA, Congress sought to validate the "gut feeling" that people ought to be able to read books and watch films privately, without that information being shared. *Id.* (quoting Rep. McCandless). The videos we choose to watch can reveal preferences and interests that we may wish to keep private. Without assurances of such privacy, our freedom to consume media is considerably curtailed.

Congress's concern was not limited just to public disclosure, but also to the sort of data aggregation, selling, and brokering that has become all too common in the online ecosystem today. Even in 1988, the legislative history shows that lawmakers were aware of the "new, more subtle and pervasive form of surveillance" that is "the trail of information generated by every transaction that is now recorded and stored in sophisticated record-keeping systems." *Id.* (citing 134 Cong. Rec. S5401 (May 10, 1988)). They recognized that when these systems monitor Americans' consumption of media such as video content, these "'information pools'" raise privacy concerns "that directly affect the ability of people to express their opinions, to join in association with others, and to enjoy the freedom and independence that the Constitution was established to safeguard." *Id.* (citing 134 Cong. Rec. S5401 (May 10, 1988)).

Congress knew about these risks, and they passed the VPPA to provide a special shield to customers' video-viewing data. Indeed, the Act's authors anticipated how technological advances like the advent of the computer could create "the ability to be more intrusive than ever before," as "[e]very day Americans are forced to provide to businesses and others personal information without having any control over where that information goes." *Id.* at 6–7 (quoting 134 Cong. Rec. S5401 (May 10, 1988)). The statute was carefully and deliberately written broadly in order to adapt to those changes. One sponsor explicitly stated on the Senate floor that the law was crafted to "strike[] the necessary balance to ensure that our privacy will not be lost as we move ahead [in developing new technologies]." 134 Cong. Rec. S5401 (10262) (statement of Sen. Simon). And even though Congress has not yet

completed the task of providing similarly robust protection to other types of data, the rapid expansion of these tracking techniques has made the VPPA more important than ever.

The Act's importance was reaffirmed when, in 2013, Congress updated it "to reflect the realities of the 21st Century," 158 Cong. Rec. H6850 (Dec. 18, 2012) (statement of Rep. Goodlatte), in what was commonly referred to as the "Netflix Amendment." Yana Welinder, *Dodging the Thought Police: Privacy of Online Video and Other Content Under the 'Bork Bill'*, Harv. J.L. & Tech. Digest (Aug. 14, 2012);[3] *Netflix Social Sharing Bill Passes Without Email Privacy Protection*, Huffington Post (Dec. 26, 2012).[4] During debates over the amendment in 2012, lawmakers repeatedly emphasized the importance of preventing the unauthorized disclosure of video-viewing information in the internet age. *See* 158 Cong. Rec. H6849–52 (Dec. 18, 2012) ("It's time that Congress update the VPPA to keep up with today's technology and the consumer marketplace. This bill does just that.").

In other words, in 1988, and again in 2013, Congress recognized the uniquely sensitive nature of video-viewing records, especially in light of technology/internet-enabled surveillance practices. The fundamental purpose of the Act is clear: to allow Americans to consume audiovisual media without the inhibition of fearing that details about their desires and

---

[3] https://jolt.law.harvard.edu/digest/dodging-the-thought-police-privacy-of-online-video-and-other-content-under-the-bork-bill.

[4] https://www.huffpost.com/entry/netflix-social-sharing-bill_n_2367385.

behaviors might be provided to others without their consent. *See* Richards, *supra* at 58.

B. The VPPA's purpose is served by protecting all video-viewing records held by providers, regardless of whether the customer subscribes to videos.

The interest in watching videos without inhibition or fear of disclosure applies whenever a consumer requests or obtains video materials from a provider. It does not hinge, as the lower court's atextual interpretation suggests, on whether the commercial relationship between the consumer and the provider is primarily related to those audiovisual materials.

Congress's focus in enacting the VPPA was on stopping providers—who hold unusually sensitive information about Americans—from disclosing that information about a person to others without the person's consent. It is hard to believe Congress would have meant to leave the video-viewing records of some consumers unprotected simply because they purchased, subscribed to, or rented the wrong type of good or service from a provider.

What makes far more sense is that Congress intended to apply the Act's protections to consumers who have a commercial relationship with the provider. This relationship distinguishes consumers from random members of the public, employees of the provider, and other individuals who do not have the same type of contractual relationship with the provider. When a person rents, buys, or subscribes to goods or services of *any* kind from a provider, the company is likely to obtain personal information about that person (such as their name and address) that it would not otherwise have. In doing so, the consumer puts their trust in the

provider to protect this information, and the provider benefits from the transaction either through a monetary payment or through growing its subscriber base.[5]

This specific commercial relationship does two things that justify imposing greater restrictions on the provider. First, it substantially increases the harm that can be caused by unauthorized disclosure of the person's video-viewing records. The more information about the viewer that a company can tie the video-viewing records to, the more sensitive those records become. Second, it justifies imposing a special duty on the provider. The provider acquired this information as part of a transaction from which it benefited, and the customer put their trust in it. It is reasonable to demand more from a provider in this circumstance—specifically, demanding that they avoid unauthorized disclosure of video-viewing data—than might otherwise be appropriate. Given the Act's history and purpose, this is the most logical and coherent distinction between those Congress would wish to apply VPPA protections to and those it would not. The statute's purpose thus justifies reading "consumer" to mean a person who subscribes to *any* product or service of a provider.

---

[5] Marketing firms recognize the inherent value of a large subscriber base for business growth. *See, e.g.*, Procept Marketing, *5 Powerful Reasons Why Mailing Lists Are Essential for Business Growth* (Nov. 6, 2024), https://proceptmarketing.com/power-of-mailing-lists/ (noting that allows for cost-effective marketing by "encouraging customers to subscribe . . . open[s] the door to sharing promotions, sales, and valuable information," provides insights into customer preferences, and increases customer loyalty).

An example can be illustrative here. Let us bring the Judge Bork case into the 21st Century and imagine that he had instead subscribed to Google's email services, creating an account in the process. The Judge then watched videos on YouTube (a Google subsidiary). These videos are readily accessible to the public; they do not require a Google account to access, and the Judge never created a separate account to access these videos. However, because Google uses the same accounts across all its services, he was logged in while watching the videos and all videos viewed were tied to his Google account. If Google gave to a journalist a list of all YouTube videos Judge Bork had viewed, it is hard to imagine that Congress would have been any less outraged. What likely *would* leave the 1988 Congress outraged (and the 2012 Congress too, for that matter) is the notion that the VPPA might *not* give the Judge a cause of action in such an instance. Yet this is precisely the interpretation the Sixth Circuit has taken here.

Mr. Salazar subscribed to a non-audiovisual service of 247Sports (a Paramount subsidiary), providing his email address to 247Sports and providing 247Sports a benefit. He then obtained specific video materials from 247Sports; the company disclosed information that identified Mr. Salazar's request for those videos to a third party. From the standpoint of the VPPA's purpose, this is materially no different than if Mr. Salazar had directly subscribed to an audiovisual service from 247Sports. In both instances, the result of this disclosure is a breach of trust that leaves the individual unable to view videos privately. Interpreting the Act in a way that would deny Mr. Salazar protections is directly contrary to the statute's purpose.

C. A broad reading of "consumer" under the VPPA tracks ordinary meaning and is consistent with the law's structure.

The definition of "consumer" as a renter, purchaser, or subscriber of *any* good or service from a VTSP is not only most consistent with Congress's purpose for the VPPA, but also the most natural reading of the text. The Act defines "consumer" as "any renter, purchaser, or subscriber of goods or services from a video tape service provider." 18 U.S.C. § 2710(a)(1). The definition makes no mention of *audiovisual* goods and services specifically, and the Court should thus assume the term is not so limited.

The definition's lack of an audiovisual limitation is hardly so surprising as to justify judicial rewriting. On the contrary, as written, the statute's definition of "consumer" is nearly identical to the term's ordinary meaning—both at the time and today. *See e.g.*, *Consumer*, Oxford English Dictionary (2d ed. 1989) ("one who purchases goods or pays for services"); *Consumer*, Webster's Third New Int'l Dictionary 573 (1986) ("one that utilizes economic goods").

Viewing the definition in the context of the statute's other definitions reinforces this interpretation. Congress "knew to include an audiovisual limitation in the VPPA when it wanted one to apply." *Salazar v. NBA*, 118 F.4th 533, 547 (2d Cir. 2024). The Act defines "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* . . . ." 18 U.S.C. § 2710(a)(4) (emphasis added). It similarly refers to "specific video materials or services" in the definition of "personally identifiable

information." 18 U.S.C. § 2710(a)(3). A natural reading shows that the term "consumer" is limited insofar as it only applies to goods and services obtained *from a provider*, but is not limited in terms of the specific type of goods and services purchased, rented, or subscribed to. For example, an individual who purchased a candy bar at Blockbuster is a consumer under the VPPA. And if that individual asked the clerk about the availability of a specific movie, a record of that person's request would be covered under the statute.

The structure of the Act further supports this straightforward textual reading of "consumer." The statute prohibits a provider from disclosing the personally identifiable information ("PII") of a consumer to a third-party, unless consent has been obtained or an exception applies. The PII definition is already limited to "information which identifies a person as having requested or obtained specific video materials or services form a video tape service provider." 18 U.S.C. § 2710(a)(3). Artificially restricting the "consumer" definition to also be limited to audiovisual materials would render this limitation in the PII definition superfluous. Such readings are strongly disfavored. *See TRW Inc. v. Andrews*, 534 U.S. 19, 31 (2001).

The lower court dismissed this structural argument on the basis that the PII definition uses the term "includes" rather than "means," suggesting it is not truly limited to video materials or services. *See* Pet. App. 17a. The legislative history indicates otherwise, however. The Senate Report, in clarifying the statute's meaning, explains that the definition of PII "includes the term 'video' to make clear that simply because a business is engaged in the sale or rental of video materials or services does not mean that all of its products

or services are within the scope of the bill." S. Rep. No. 100-599, at 12 (1988). The Report goes on to explain that the definition "is intended to be transaction-oriented," covering only "information that identifies a particular person as having engaged in a specific transaction with a video tape service provider." *Id.*

Much ink has been spilled, of course, over how much weight should be given to such comments in legislative history. But when the plain text *and* legislative history both strongly support the same interpretation, it would be ill-advised to reject that interpretation on the grounds that a judicial rewrite of the statute is needed to effectuate Congress's will.

Indeed, the statute works most effectively when the definition of "consumer" is interpreted broadly, consistent with its plain meaning. The law's other provisions already adequately limit the statute's scope to the type of video-viewing data that Congress sought to protect. The definition of video tape service provider limits the Act's restrictions so they only apply to companies engaged in a specific course of business. Likewise, the definition of PII focuses the restrictions on protecting information that identifies a person as having requested or obtained specific video materials or services. It is hard to imagine any scenario where a provider covered by the Act is disclosing PII as defined under the Act but that disclosure is not the sort that Congress sought to restrict.

In enacting the VPPA, Congress recognized "that individuals should be protected in their personal use of videotapes" and similar services. 134 Cong. Rec. S5400 (10261) (Sen. Grassley). Where a provider keeps information about the videos a person requests or obtains from them, the provider should owe a duty to

keep that information safe whenever there is a consumer-provider relationship, not only when the consumer subscribed to audiovisual services specifically.

II. Adopting a natural reading of "consumer" will not stop VTSPs from providing video services or serving advertisements.

The premise underlying Paramount's argument in this case—that a natural reading of the term "consumer" would "transmogrify [the VPPA] into a prohibition against targeted advertising on the Internet," Br. Opp. Cert. 1—is false. Applying the VPPA's protections to all consumers of a VTSP's goods or services, as the Act's text and purpose both support, would simply prohibit the disclosure of personal video-viewing information without affirmative consent. It would not prohibit advertising, or the targeting of advertising, at all. No matter how "consumer" is defined, providers will be able to use the tools and systems necessary for their websites to function and provide services, as well as to display, and even target, advertisements. Indeed, other companies that are subject to the VPPA are currently serving and targeting advertisements without disclosing personal video-viewing information to third parties. *See Privacy Statement*, Netflix (Apr. 10, 2026) (specifying that they do not "share information about title selections of shows or movies you have watched on our service").[6]

A. Online tracking tools that disclose video-viewing data to third parties are not necessary for providing video services.

The VPPA restricts providers' use of online tracking tools—such as the Meta Pixel used by

[6] https://help.netflix.com/legal/privacy.

Paramount here—that send consumers' protected video-viewing information to a third party (here, Meta) without consent. But it is important to note that the Act does *not* prohibit providers from using the sorts of online tracking tools—even cookies and pixels—that are necessary for services' functionality. This is because the VPPA regulates disclosure of information, not collection of data, and these tools are used in many ways that do not involve sending video-viewing data to third parties.

As an initial matter, it is helpful to explain how these tools, specifically cookies and pixels, work. In brief, a cookie is a small file set by a website's server and stored on a user's device by their browser for retrieval later. *Online Profiling: A Report to Congress*, Fed. Trade Comm'n (June 2000).[7] A pixel is a small image or other piece of code embedded on a webpage that can collect data and track certain user behaviors, such as pageviews, clicks, and interactions with ads. *Lurking Beneath the Surface: Hidden Impacts of Pixel Tracking*, Fed. Trade Comm'n Office of Tech. (Mar. 16, 2023).[8]

Cookies and pixels can be used to improve a website's functionality. For example, single-session cookies (which expire as soon as a user closes the web browser) allow a website to keep track of a user's identity as they browse different pages on the site. *Maintaining Session State with Cookies*, Microsoft (June 15,

---

[7] https://www.ftc.gov/sites/default/files/documents/reports/online-profiling-federal-trade-commission-report-congress-part-2/onlineprofilingreportjune2000.pdf.

[8] https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2023/03/lurking-beneath-surface-hidden-impacts-pixel-tracking.

2017).[9] These cookies can make it possible for a user to stay logged into their account for the duration of a website-visit, rather than requiring them to log in each time they access a new page. Similarly, on e-commerce websites, these cookies can be used to store the items a user adds to their shopping cart. John Schwartz, *Giving Web a Memory Cost Its Users Privacy*, N.Y. Times (Sept. 4, 2001).[10] It was difficult to enable this type of function without cookies in the early days of the internet; a website would have no way of knowing the user who added an item to the cart was the same person now accessing the checkout page. "Persistent cookies," which stay on a user's device for a longer period, can also serve a functional purpose, such as remembering a user each time they return to a website rather than requiring to log back in at the start of each new visit. *Maintaining Session State with Cookies*, Microsoft, *supra*. Pixels, too, can be functional, helping websites with analytics or language preferences, for example.

The VPPA does not restrict providers' use of these tools for collecting or using data, no matter how "consumer" is defined. The Act regulates the non-consensual disclosure of data, not its collection. When a provider is collecting data for its own use, the Act's disclosure prohibition is simply not implicated.

But since the early days of the commercial internet, digital advertising companies have sought to use online tracking tools to profile users based on their behaviors and inferred interests to facilitate targeted

---

[9] https://learn.microsoft.com/en-us/previous-versions/iis/6.0-sdk/ms526029(v=vs.90)?redirectedfrom=MSDN.

[10] https://www.nytimes.com/2001/09/04/business/giving-web-a-memory-cost-its-users-privacy.html.

advertising. *Surfer Beware: Personal Privacy and the Internet*, EPIC (June 1997).[11] Indeed, once it became common to use persistent cookies to identify users, some firms began using those identifiers to track user behavior across different websites and services in order to build a deeper record of user activity.

As awareness of these surveillance tactics became widespread, a growing proportion of consumers, looking to protect their privacy, sought out tools to block these persistent, non-necessary cookies. This led to a sort of tracking arms race, leading some firms to look for other tools to track users' browsing habits in ways that were harder to block. Tracking pixels became popular for this purpose. These pixels can be used to collect large amounts of personal data, including user clicks, viewing history, and direct identifiers like email addresses, all while remaining difficult for most users to detect. By their nature, they operate invisibly, and users typically cannot block tracking pixels without disabling the downloading of all images on a website, which would seriously impair functionality. It is these uses of cookies and pixels to track users that can potentially implicate the VPPA.

While some website operators use tracking pixels to collect data themselves (a practice the VPPA does not restrict), more commonly these pixels are included in third-party plug-ins or features that the website operator adds to their webpage. With these third-party pixels (or other third-party tracking technologies), information about each user who visits the page is not merely stored by the website operator: it is disclosed by the provider to a third party.

---

[11] https://archive.epic.org/reports/surfer-beware.html.

Users are largely unaware of these data disclosures. While it is clear when a user requests or loads a page that they are communicating with—and providing some information to—the operator of the website, the same is not true for the third-party entity whose invisible pixel is embedded on the page.

The Meta Pixel, formerly called the Facebook or "FB" pixel, used by Paramount in this case, is the most widely used tracking pixel and is integrated by websites to collect detailed navigation histories of their users, among other data. Paschalis Bekos et al., *PIIxel Leaks: Passive Identification of Personally Identifiable Information Leakage through Meta Pixel*, CCS '25 (Oct. 2025).[12] The pixel conveys this information to Meta, which can then match website visitors to people who use Meta platforms in order to build "custom audience[s]" for targeted advertising. *About Advanced Matching for Web*, Meta (last visited Apr. 9, 2026).

The amount of data that companies collect and disclose with these pixels is significant. Researchers have found that the Meta Pixel can track "how far down a page a user has scrolled, whether a user has reset their password, and if a user viewed the video on the page[.]" Surya Mattu & Aaron Sankin, *How We Built a Real-time Privacy Inspector*, Markup (Sept. 22, 2020). The pixel also tracks "any buttons clicked by site visitors, the labels of those buttons and any pages visited as a result of the button clicks." *Meta Pixel*, Meta (last visited Apr. 9, 2026).[13] It can even collect information entered in forms, like a user's email and

---

[12] https://dl.acm.org/doi/epdf/10.1145/3719027.3765113.

[13] https://developers.facebook.com/docs/meta-pixel/.

home address, when a user types them in on a site. Mattu & Sankin, *supra*.

This information can provide a detailed view of a person's viewing habits. In many cases, the page a user has loaded reveals specific video content that they are requesting and obtaining. In these circumstances, as in this case, Meta can link the user with a specific video they have watched. When a video is at the bottom of a page and requires a click to start, a Meta Pixel can likewise record that the user scrolled to the bottom, pressed start, and stayed at the bottom of the page watching. And because Meta uses "Advanced Matching" to link its pixel's tracking data with a user's identity—even when the user does not have, or is not logged into, a Facebook account—it can identify the specific person watching the video. Mattu & Sankin, *supra*. In this way, the companies that embed the Meta Pixel on their website disclose exactly the type of personal information that the VPPA regulates.

It is crucial to distinguish these third-party tracking tools from those that are necessary to a VTSP's website's functionality. While some amount of data must be processed to operate a website, there is no actual need for a provider to deploy third-party tracking technologies that siphon personal data from visitors and send it to a company like Meta.

In fact, many website operators have declined to include the Meta Pixel on, or have taken it off, their sites without sacrificing the integrity of their operations. The Department of Education stopped using the Meta Pixel after an investigation revealed that it had collected names, email addresses, and zip codes of prospective college students who filled out the Free Application for Federal Student Aid (FAFSA) form on the

Department's website. Surya Mattu & Colin Lecher, *Applied for Student Aid Online? Facebook Saw You*, Markup (Apr. 28, 2022).[14] Likewise, several hospitals removed the Meta Pixel from their appointment scheduling pages and patient portals after another investigation revealed that the pixel sent highly sensitive information to Meta, including names of patients and doctors, reasons for appointments, and information about prescriptions. Todd Feathers et al., *Facebook Is Receiving Sensitive Medical Information from Hospital Websites*, Markup (June 16, 2022).[15] The Department of Education's FAFSA online form is fully functional without the Meta Pixel, as are the websites of hospitals that elected to remove it.

In other words, the Meta Pixel is not necessary for a website to operate, and website operators—including VTSPs—are able to remove the pixel to protect their users' sensitive information or to comply with the law. Providers' use of third-party tracking tools is not a technological or economic necessity, let alone one that warrants judicially rewriting an important federal privacy statute like the VPPA.

B. The restrictions of the VPPA do not prevent a provider from serving advertisements.

Though the VPPA limits providers' ability to non-consensually disclose users' personal data to third parties, inhibiting some of the mass data disclosures

---

[14] https://themarkup.org/pixel-hunt/2022/04/28/applied-for-student-aid-online-facebook-saw-you.

[15] https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites.

that power the targeted advertising ecosystem, providers still have many lawful avenues to serve effective—even targeted—advertisements. Providers can freely engage in contextual advertising or use first-party data to target ads. They can even disclose a user's personal data for further targeting, they simply must obtain valid informed consent first. There is no need to artificially narrow the meaning of the term "consumer" to protect online advertising, consequently.

Most significantly, providers can effectively target advertisements without disclosing VPPA-protected personal data to third parties by instead using information they already know about their customers. This is known as first-party targeted advertising. Param Gopalasamy, *Mastering First-Party Data: The Complete Playbook for Marketers*, OneTrust Blog (last visited Apr. 21, 2026).[16] Providers like Paramount are well positioned to do this sort of targeting as, even without relying on third parties, they have ample data from which to identify their users' interests. A provider is free under the VPPA to use the various videos a consumer has watched to tailor advertisements that are most likely to match their interests. The only thing the VPPA limits is providers' disclosure of that video-viewing data to others.

The VPPA also does not restrict providers' ability to engage in contextual advertising. This is again true no matter how "consumer" is defined. Contextual advertising uses the context in which an advertisement is shown—as opposed to the persistent personal data of the viewer—to target advertisements. With contextual advertising, the advertisements shown are

---

[16] https://www.onetrust.com/blog/mastering-first-party-data-the-complete-playbook-for-marketers/.

based on the content of the webpage where the ad is displayed, the nature of the audience likely to consume that content, or even the search string that led a viewer to that page. *See Contextual Advertising*, Amazon Ads (last visited Apr. 9, 2026).[17] This can be very effective. If a user searches "best winter jacket for freezing temperatures," for example, it is possible to serve a highly relevant contextual ad for winter jackets on the search results page without relying on any personal data of the user.

In this case, Paramount could easily have used contextual advertising to provide relevant advertisements to its subscribers without using the Meta Pixel. 247Sports is a specialty sports content website. Visitors to the website are presumably interested in sports, and so advertisements for sports equipment, memorabilia, or team merchandise are likely to be relevant. In this way, the contextual advertising model—which carries into the digital space the dominant advertising paradigm across most of human history—allows for effective audience penetration without violating consumers' privacy rights.[18] In other words, even when the VPPA's disclosure regulations limit providers ability to engage in certain types of targeted advertising, these companies still have ample options to display and target advertisements effectively. There is no

---

[17] https://advertising.amazon.com/library/guides/contextual-advertising.

[18] "The big ad-tech companies know how to sell ads without damaging privacy, but they choose not to." Gabriel Weinberg, Opinion, *What if We All Just Sold Non-Creepy Advertising?*, N.Y. Times (June 19, 2019), https://www.nytimes.com/2019/06/19/opinion/facebook-google-privacy.html.

need to curtail the law's reach to minimize its impact on providers' advertising practices when so many alternatives already exist.

Finally, it is important to note that, to the extent providers want to continue to disclose personal viewing data to a firm like Meta, the VPPA only requires that they first obtain a consumers' affirmative consent. The Act does not prohibit all such disclosures (though some other privacy laws do). It should not be surprising to a provider like Paramount that they must seek affirmative consent before disclosing a user's sensitive data to a third party. Businesses across many other industries, including health care and finance, must obtain valid consent before disclosing sensitive personal information, even when those businesses may find this requirement inconvenient.

This Court should not atextually narrow the statute's definition of "consumer" merely because it imposes a modest burden on providers to obtain written, informed consent before disclosing personally identifiable information—especially when Congress already modified the VPPA consent provisions in 2013 to be readily applicable to the internet age.

It is likely that many consumers do not want their video providers to disclose their personal video-viewing data to third parties for the purpose of targeted advertising. That is exactly the situation the VPPA was designed to address, and it would be backwards to use likely consumer opposition to tracking as evidence that there should be a carveout within the definition of consumer. Congress passed the VPPA to protect Americans' video-viewing data. If Americans make the choice not to allow providers to share their

data it is not a defect with the statute; that would be the statute working exactly as intended.

Restricting the disclosure of consumers' video-viewing data does not threaten to jeopardize the financial wellbeing of VTSPs. Indeed, these firms are far more profitable today than they were when Congress first enacted the VPPA. In 1988, Blockbuster had only been around for three years and had 800 stores. By its peak in 2004, it made $5.4 billion in revenue with 9,000 stores globally. Frank Olito & Alex Bitter, *Blockbuster: The Rise and Fall of the Movie Rental Store, and What Happened to the Brand*, Business Insider (Apr. 24, 2023).[19] The estimated worldwide revenue of on-demand video streaming services is set to reach almost $100 billion in 2026, *Video Streaming (SVoD) – Worldwide*, Statista (last visited Apr. 23, 2026),[20] and is expected to grow to $200 billion by 2030. Grace Harmon, *Ad-Supported Tiers Power a $150 Billion Global Streaming Market*, EMarketer (Apr. 2, 2026).[21]

The growth in the streaming video marketplace has made the VPPA more important than ever. And this trend has coincided with a proliferation of online tracking technologies. All consumers, regardless of what product or service they subscribe to or purchase, should feel confident—as the VPPA's text promises—that the videos they watch will remain private. This

---

[19] https://www.businessinsider.com/rise-and-fall-of-blockbuster#despite-the-rise-of-netflix-and-redbox-blockbuster-was-at-its-peak-in-2004-10.

[20] https://www.statista.com/outlook/amo/media/tv-video/ott-video/video-streaming-svod/worldwide?currency=USD#revenue.

[21] https://www.emarketer.com/content/ad-supported-tiers-power-150-billion-global-streaming-market.

was Congress's goal when it originally enacted the statute, and the technological and market changes over the last four decades have not changed that goal. This Court should not curtail the Act's scope, at the expense of consumers, simply because some providers wish to monetize their users' sensitive personal data.

CONCLUSION

For the above reasons, amici respectfully ask this Court to vacate the judgment of the Court of Appeals for the Sixth Circuit and remand for further proceedings consistent with the Court's opinion.

Respectfully submitted,

ALAN BUTLER
Counsel of Record
JOHN DAVISSON
THOMAS MCBRIEN
SARA GEOGHEGAN
HAYDEN DAVIS

ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC)
1519 New Hampshire
Avenue NW
Washington, DC 20036
(202) 483-1140
(202) 483-1248 (fax)
butler@epic.org

April 24, 2026