No. 25-459

In the Supreme Court of the United States

MICHAEL SALAZAR,
Petitioner,
v.
PARAMOUNT GLOBAL, DBA 247SPORTS,
Respondent.

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE SIXTH CIRCUIT

BRIEF OF META PLATFORMS, INC. AS *AMICUS CURIAE* IN SUPPORT OF RESPONDENT

MELANIE BLUNSCHI
NICHOLAS ROSELLINI
LATHAM & WATKINS LLP
505 Montgomery Street
Suite 2000
San Francisco, CA 94111

NIKKI STITT SOKOL
CARRIE J. BODNER
META PLATFORMS, INC.
1 Hacker Way
Menlo Park, CA 94025

ROMAN MARTINEZ
Counsel of Record
ANDREW B. CLUBOK
SUSAN E. ENGEL
SOREN J. SCHMIDT
RUTH HIRSCH
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004
(202) 637-3377
roman.martinez@lw.com

Counsel for Amicus Curiae *Meta Platforms, Inc.*

TABLE OF CONTENTS

Page

TABLE OF CONTENTS—Continued

Page

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES—Continued

Page(s)

TABLE OF AUTHORITIES—Continued

Page(s)

TABLE OF AUTHORITIES—Continued

Page(s)

FEDERAL STATUTES

TABLE OF AUTHORITIES—Continued

Page(s)

STATE STATUTES

TABLE OF AUTHORITIES—Continued

Page(s)

OTHER AUTHORITIES

TABLE OF AUTHORITIES—Continued

Page(s)

TABLE OF AUTHORITIES—Continued

Page(s)

INTEREST OF *AMICUS CURIAE*

Founded in 2004, Meta Platforms, Inc. is a technology company dedicated to helping people build communities and to bringing the world closer together.[1] Meta's services, which include Facebook and Instagram, are used by billions of people worldwide. And Meta's suite of analytics tools, including Meta's Pixel code (for websites) and Software Development Kits (for mobile apps), are used by millions of website and app developers to help them understand user activity, improve their products and services, and tailor advertising efforts.

Meta has a significant interest in this case, which involves allegations related to one developer's use of Meta's Pixel code. Salazar alleges that 247Sports violated the VPPA by incorporating this code into its website and using it to gather information about video content he viewed on 247Sports' website and transmit that information to Meta. This lawsuit is part of a recent wave of litigation seeking to punish the companies who provide modern analytics tools—and the millions of developers who depend on them—by distorting the text of inapposite federal and state statutes. Meta seeks to clarify the purpose, functionality, and benefits of these technologies, and to explain how correctly interpreting the VPPA can help stem the tide of these meritless lawsuits.

---

[1] No counsel for any party authored this brief in whole or in part, and no party, counsel for a party, or person or entity other than *amicus curiae* and its counsel made a monetary contribution intended to fund the brief's preparation or submission.

INTRODUCTION AND SUMMARY OF ARGUMENT

The core issue in this case is whether the Video Privacy Protection Act (VPPA)—a Blockbuster-era statute enacted in 1988 to protect video tape rental records—can be stretched to regulate pixel technology that helps modern websites analyze user activity. It cannot. This Court should affirm, for the reasons respondent has set forth.

Meta submits this amicus brief to emphasize two important points that should inform the Court's resolution of this case.

First, pixel technology and similar analytics tools play a vital role in today's online ecosystem. Many companies, including Meta, make pixel code available for developers—i.e., website owners and operators—to customize and use. Pixel code is a ubiquitous and highly important feature of the modern internet, something millions of developers across every industry—including small businesses and charitable organizations—use to analyze how users interact with their websites. Developers choose whether and where to incorporate Meta's Pixel code on their website, consistent with their contractual obligations to Meta and their users. They can also customize the code to analyze the user interactions they care most about, subject to those same obligations. Pixel technology enables a wide range of beneficial uses, from improving websites to delivering relevant advertisements. Meta's Pixel code is one of several similar tools that Meta makes publicly available for developers to use free of charge, complete with robust privacy protections, contractual requirements, and user safeguards.

Second, this case is just one salvo in an ongoing broadside attack on modern analytics tools. In recent years, hundreds of putative class action lawsuits have been filed against companies (like Meta) who provide pixel technology and the many developers (like 247Sports) who depend on it. Unable to identify any law that actually prohibits this ubiquitous technology, plaintiffs have resorted to an array of inapposite statutes—including federal and state criminal prohibitions on wiretapping, anti-hacking statutes, and now the VPPA—to seek eye-popping statutory damages awards. Some courts have blessed those efforts, casting a pall of uncertainty over routine website development and online marketing practices. This Court, however, has roundly rejected previous attempts to distort statutory text in service of penalizing commonplace uses of modern technology. Instead, the Court has repeatedly reaffirmed the importance of faithfully adhering to statutory text, respecting legislative limits on liability, and fostering the development and use of modern technologies.

The Court should take that same approach here, where the VPPA cannot support Salazar's claims. Salazar alleges that 247Sports, an athletics website, violated the VPPA by using Meta's Pixel code to share his Facebook ID and certain web activity data with Meta. Pet. App. 91a-95a (¶¶ 30-40). But the VPPA bars only "video tape service provider[s]" from disclosing "personally identifiable information" about the video rental history of any "consumer"—i.e., a "renter, purchaser, or subscriber of goods or services from a video tape service provider." 18 U.S.C. § 2710(a)-(b). That carefully targeted statutory text does not fit the facts of this case. And nothing in the VPPA remotely suggests that Congress prohibited

using pixel technology to analyze user activity on every website that happens to include video content.

Rebuffing Salazar's claims will set a valuable example for other courts mired in litigation challenging pixel technology and other analytics tools. It will remind courts that statutory text should not be contorted in service of penalizing commonplace uses and distribution of modern technology. And it will encourage them to reject boundless constructions of numerous laws frequently deployed in misguided attacks on pixel technology.

ARGUMENT

I. MODERN ANALYTICS TOOLS LIKE PIXEL TECHNOLOGY PLAY A VITAL ROLE IN TODAY'S ONLINE ECOSYSTEM

In the digital marketing context, developers rely on modern analytics tools to analyze user activity, which in turn helps them improve their products, services, and advertising efforts. A "pixel" is a snippet of computer code that developers can incorporate into their websites to analyze users' online activity. Similar analytics tools exist for mobile apps.

This case concerns a version of pixel technology that Meta developed and makes freely available for websites to use according to their needs. Salazar alleges that 247Sports used Meta's Pixel code to transmit certain web traffic data, supposedly in violation of the VPPA. Developers of websites like 247Sports choose whether and how to incorporate Meta's Pixel code, which individual webpages will contain that code, what kinds of user activity will be measured and transmitted to Meta, and what information will (or will not) be shared with Meta.

Given the wide diversity and sheer scale of Meta Pixel code usage, Meta has established robust policies, contractual requirements, and technical systems designed to prevent receipt and use of potentially sensitive user data that developers could choose to transmit. As it considers Salazar's claims challenging 247Sports' use of Meta's Pixel code, the Court should understand how Meta strives to safeguard data privacy while supporting developers, advertisers, and users.

A. Pixel Technology Benefits Millions Of Developers And Their Users

Millions of websites—including many of the highest-traffic websites on the internet—use pixel technology. And hundreds of thousands of mobile apps use similar analytics tools. That widespread adoption reflects the significant benefits that these technologies generate for developers, advertisers, and everyday people across the world.

The core purpose of pixel technology and other modern analytics tools mirrors the marketing and recordkeeping practices that businesses, non-profits, and other organizations have long used to attract and retain customers and supporters. For example, at brick-and-mortar stores, shopkeepers observe where their customers are spending the most time or how they move through the store. These observations can inform the store's decisions on how best to display inventory or organize the store to encourage more purchases. Or, if a customer signs up for a rewards program, the store might keep track of the customer's purchases and send them a coupon to encourage similar purchases in the future. Such practices

inform strategic decisions and facilitate personalized communication.

Modern analytics tools, including pixel technology, enable the same kind of tailored outreach online. When consumers visit a website, the developer can use pixel code to help analyze their interactions with the website, such as when they view a page or make a purchase. *See About Meta Pixel*, Meta, https://www.facebook.com/business/help/742478679120153 (last visited June 30, 2026). Rather than building their own analytics tools from scratch, developers often rely on analytics tools provided by other companies. Meta's Pixel code is just one example designed for websites; others include Google Analytics, LinkedIn Insight Tag, and Adobe Analytics. Still more analytics tools, such as some of Meta's Software Development Kits (SDKs), provide similar analytics capabilities for mobile apps.

Analytics tools like pixel technology help developers in several ways. For starters, developers can use pixel technology to understand and evaluate user activity on their website, including by assessing the popularity and functionality of particular content, features, and products. For instance, an online footwear outlet might learn that customers prefer to shop for shoes by style rather than by brand, which in turn could justify creating a style filter for the website's search function. Or the developer might learn that shoe shoppers are more likely to click on a recommendations banner at the top of the page, rather than one on the left-hand side.

In this way, pixel technology gives developers valuable insights into which elements of their websites are popular and useful—and which are not. That is a good thing: The more efficient and

user-friendly an interface, the better the website will serve the developer's business or mission.

Developers can also use what they learn about user activity on their website to inform how they advertise their products, services, or activities. Many websites and web developers "make[] money through advertising." Resp. Br. 11 (comparing 247Sports to "many websites that provide content outside a paywall"). Knowing how users interact with a website helps developers understand which people will be most receptive to digital marketing elsewhere—and what products, services, or activities will interest them. For instance, a charitable foundation that targets advertisements to existing donors may also want to solicit contributions from people who have visited the foundation's website but who have not previously donated. Pixel technology helps the foundation focus its external advertising efforts on those target audiences. And it can enable the foundation to gauge which messages resonate most by tracking which advertisements get clicks and lead to donations.

The insights made possible by pixel technology are especially important for businesses, organizations, and people with limited financial resources. A local artist selling paintings online, for example, may not be able to afford a mass advertising campaign to the general public. But because of pixel technology, the artist can advertise directly to a smaller set of people who have previously viewed paintings on his website—a targeted approach that will be more effective and more affordable.

Consumers benefit from pixel technology too. Rather than being bombarded with random and irrelevant advertisements, consumers receive

outreach about products, services, and causes that they might actually be interested in buying or supporting. And because pixel technology gives small businesses an affordable way to market themselves, users enjoy more competition for the things they care about—meaning more options, lower prices, and better quality. In addition, because the revenue from these targeted advertisements supports services like Facebook, Instagram, Google, and LinkedIn, pixel technology ensures that users can continue to use those services free of charge. More generally, websites crafted with the benefit of analytics information provided by pixel technology can offer a better and more user-friendly experience.

In short, thanks to pixel technology, organizations of all stripes can more effectively invest in website development and online advertising. And people everywhere enjoy a richer, more streamlined, and more personalized online experience.

B. Countless Developers Configure Meta's Pixel Code To Suit Their Needs

Like other versions of pixel technology, Meta's Pixel code is a snippet of computer code that Meta offers to the public for free. Developers can choose to incorporate the Pixel code into their websites, as 247Sports allegedly did here. That code enables developers to gain insights into how users interact with their websites. Based on their unique needs and circumstances, developers decide what data they want to transmit to Meta, and Meta in turn provides free, developer-friendly tools for measuring and analyzing user activity. But developers are under no obligation to use any of those options, and they can customize the Pixel code to suit their needs and goals,

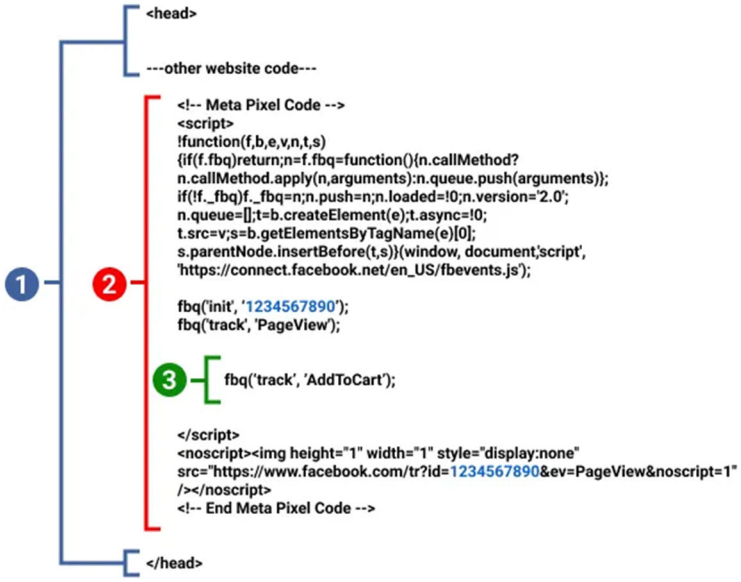
subject to their contractual obligations to Meta and their users.

Developers typically configure Meta's Pixel code to track discrete website visitor actions—i.e., "events" that occur on their websites. "Automatic Events" and "Standard Events" are interactions predefined by Meta that can be used to track user activities that may be common across many different websites. *See About automatic events*, Meta, https://www.facebook.com/business/help/1292598407460746 (last visited June 30, 2026); *About standard and custom website events*, Meta, https://www.facebook.com/business/help/964258670337005 (last visited June 30, 2026). These events can include generic actions like page views, as well as more specific actions like adding an item to a shopping cart, viewing content, starting a free trial, booking a reservation, and making a donation. *See Specifications for Meta Pixel standard events*, Meta, https://www.facebook.com/business/help/402791146561655 (last visited June 30, 2026). The Pixel code transmits Automatic Events by default, but developers can opt to disable that feature at any time. Developers can also choose whether to manually configure Standard Events themselves or instead use a setup tool that can transmit Standard Events where they appear applicable.

"Custom Events" are bespoke events created and configured by developers to measure other kinds of interactions, like when a user inputs a coupon code. *See About standard and custom website events*, *supra*. For Custom Events, what user actions are measured and what corresponding event data is sent to Meta are up to the developer.

The screenshot below shows what Meta's Pixel code looks like to developers when creating or

updating their websites. Generally, "native" code written by the developer dictates what a user's web browser will display (such as text or pictures) and how they can interact with it (such as clicking a button). Meta's Pixel code can then be added to the website's native code:



See About standard and custom website events, *supra*. The (1) blue-bracketed code is part of the website's native code. The (2) red-bracketed code is Meta's base Pixel code that developers can incorporate into their website's native code. And the (3) green-bracketed code is the Standard or Custom Event code that the developer has chosen to configure; in the above example, the developer has included the Standard Event code for "AddToCart." *Id.* Developers can manually customize Meta's Pixel code, but Meta also provides learning resources and a user-friendly

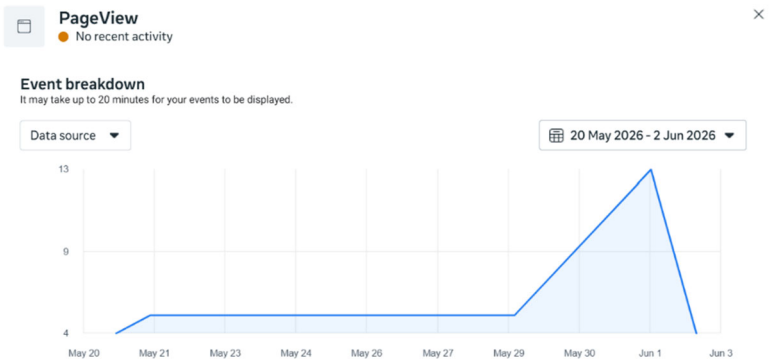
interface for developers to toggle Standard Events on or off more easily.

Where enabled, the Pixel code creates an event data point triggered by the relevant user activity and then compiles a set of event data. In this case, Salazar's complaint contains a screenshot of the raw data he alleges was gathered by 247Sports' Pixel code:

Pet. App. 95a (¶ 40). As the screenshot shows, the raw data is packaged as long strings of letters, numbers, and symbols. Salazar alleges that this data discloses "the content name of the video [he] watched, the URL, and [his Facebook ID]" when it is transmitted to Meta. *Id.*

Where developers have chosen to analyze certain user events, they typically transmit this event data to Meta, along with certain "metadata" (i.e., technical information about the user's computer or browser) and "cookies" (i.e., small text files that, among other things, allow websites to recognize repeat users). Meta then uses the data to provide free analytics services to the developers. Those analytics come in the form of anonymized, aggregated statistics about user activity.

For example, Meta helps developers assess trends in how users are interacting with the developer's own website—the pages they visited, the products they added to shopping carts, and so on. Developers can also analyze things like how many Instagram or Facebook users clicked on particular advertisements, and how many of those "click-throughs" led to actual purchases. To make the information easier for developers to understand, Meta also displays event data in graphical form. The screenshot below, for example, shows the number of page views one developer's website received over time:



These services help developers optimize their website design and marketing decisions.

Many developers rely on Meta to provide these analytics services. Meta is able to offer the technology free of charge because the event data sent by advertisers supports Meta's personalized advertising model. More specifically, as publicly disclosed in its terms and policies, Meta uses the event data from developers—who must obtain any necessary rights and permissions from users to share it, *infra* at I.C—to match the transmitted events to Facebook or

Instagram user accounts where possible. Meta can then direct advertisements—often from the same website that sent the event data—to users who allow and are most likely to be receptive to that marketing. The revenue from those advertisements allows Meta to offer services like Facebook and Instagram to users free of charge.

Throughout this process, developers of websites like 247Sports decide whether and how to use the Pixel. Meta created the Pixel code, but has made that code publicly available and free for developers to use, subject to certain contractual restrictions meant to protect user privacy. *See infra* at I.C. Incorporating Meta's Pixel code is completely voluntary, including for developers who advertise through Meta's services. Developers who do want to use Meta's Pixel code decide for themselves where (and where not) to use it. Some developers place Meta's Pixel code only on a landing page to measure advertisement click-throughs. Others incorporate it elsewhere to track a broader range of activities, such as reading an article or applying a coupon.

Developers decide what event data to transmit to Meta. As described above, tracking for all events—Automatic, Standard, and Custom—is optional. Likewise, developers can choose whether to transmit other information, including certain metadata and cookies. Developers can also choose to place preconditions on sending information. All developers make a contractual promise to Meta that they will only transmit data that they are authorized to share—and that they will not use the Pixel code to collect or share sensitive data. Many developers configure their website and Pixel code not to transmit any information unless a user has clicked "accept" on

a pop-up banner asking for consent to the website's use of analytics technology. Some users' individual settings, including ad-blocking software or private browsing modes, can also prevent certain data from being sent. What data gets sent to Meta is thus a product of decisions by millions of individual developers and website users.

C. Meta Protects User Privacy

To ensure it can be used effectively by millions of developers across virtually every industry, Meta's Pixel code is customizable. But Meta does not want developers to configure the Pixel code in ways that might transmit any sensitive data, such as health or financial information. To that end, Meta has established robust policies, contractual requirements, and technical systems designed to promote data privacy, while preserving the ability of website developers like 247Sports to use Meta's Pixel code to analyze user activity on their websites.

Recognizing that developers are best positioned to control their own websites and data transmissions, Meta requires developers to agree that they will not share sensitive information with Meta. Meta's Business Tools Terms forbid sharing any information that "includes or is based on, directly or otherwise, health information, financial information, consumer report information, or other categories of sensitive information." *See Meta Business Tools Terms* § 1(h), Meta, https://www.facebook.com/legal/technology_terms (last visited June 30, 2026). Meta also warns developers to ensure that their chosen Custom Event labels do not convey any sensitive information. *See About reviewing custom events in Meta Events Manager*, Meta, https://www.facebook.com/business/

help/344247017987537 (last visited June 30, 2026). And Meta requires developers to provide "robust and sufficiently prominent notice to users regarding [Pixel event] [d]ata collection, sharing, and usage." *Meta Business Tools Terms* § 3(c), *supra*.

In addition, Meta provides education and guidance to developers to help them protect sensitive data and obtain any needed user consent. *See, e.g.*, *About prohibited information*, Meta, https://www.facebook.com/business/help/361948878201809 (last visited June 30, 2026) (providing details on prohibited forms of sensitive information); *Cookie Consent Resource*, Meta, https://developers.facebook.com/docs/app-events/cookies/ (last visited June 30, 2026) (explaining general principles of consent and recommending vendors and industry tools to assist in obtaining consent).

If Meta discovers that a developer is nonetheless transmitting potentially sensitive information, Meta flags the issue and directs the developer to assess its practices and change them as necessary to comply with their contractual obligations. *About prohibited information*, *supra*. Failure to make the required changes may result in Meta modifying, suspending, or terminating the developer's ability to use Meta's Pixel code and accompanying analytics services. *Id.*; *Meta Business Tools Terms* § 4(a), *supra*.

Meta's technical controls are designed to detect, filter out, and (where feasible) prevent the transmission of information that developers are prohibited from sharing under Meta's terms. *See About prohibited information*, *supra*. For example, Meta devotes considerable resources to developing internal systems aimed at preventing any

unauthorized personally identifiable information from being stored and used by Meta. *See id.*

Meta also categorizes data sources—i.e., websites and apps—that share data with Meta through pixel code and other tools based on the topics related to the data source and the products and services it provides. Certain categories come with additional data sharing restrictions, which may include limiting or fully restricting the ability to share certain event data with Meta. *See About data source categories in Meta Events Manager*, Meta, https://www.facebook.com/business/help/1402913027039332 (last visited June 30, 2026). These include health and wellness, financial services, politics, race, religion, and gender or sexuality, among others.

One such control is called "core setup." *See About core setup*, Meta, https://www.facebook.com/business/help/124742407297678 (last visited June 30, 2026). Core setup prevents the transmission of custom "parameters"—i.e., additional information associated with a specific event that developers can choose to measure, such as the age of a user making a purchase or an inventory category for the item. *See id.* Core setup also truncates URL text after the domain name to help prevent the sharing of information not allowed under Meta's terms. For example, if the event data would typically contain the URL "www.yourbank.com/student_loans," core setup removes "student_loans" from the URL, leaving only "www.yourbank.com/." And for data sources in certain categories (such as healthcare and financial services), Custom Event names are subject to human review and blocked if they contain prohibited information. Core setup can be applied by Meta based on a data source's category, triggered when Meta's

systems detect that enhanced enforcement may be needed, or turned on manually by developers as a safeguard.

Collectively, these policy and technical measures are designed to establish robust protections against the sharing of information not allowed under Meta's terms. And Meta works to continually improve them. Meta's development and distribution of Pixel code thus embodies a responsible and widely beneficial approach to web analytics, not the unlawful infringement on user privacy that Salazar imagines.

II. COURTS SHOULD NOT DISTORT STATUTORY TEXT TO PUNISH THE DISTRIBUTION OR USE OF PIXEL TECHNOLOGY

In recent years, pixel technology and similar analytics tools have become favorite targets for the plaintiffs' bar. Plaintiffs have filed hundreds of lawsuits demanding massive damages awards against the millions of developers who depend on pixel technology and/or the companies who provide it. And they have threatened thousands more to come. But because no law actually prohibits using or distributing pixel technology, plaintiffs have resorted to far afield federal and state statutes banning activities like wiretapping, computer hacking, and—in this case—sharing video tape rental history.

Salazar claims that 247Sports violated the VPPA by using Meta's Pixel code to "display targeted advertising" based in part on data regarding "which videos [users] watched" on 247Sports' free website. Pet. 7. Under his view of the VPPA, using pixel technology to conduct routine web traffic analytics is unlawful whenever a user purchases or subscribes to

anything on a website that happens to contain video content. Although the Sixth Circuit rightly rejected Salazar's claims, many courts have blessed similarly tortured attempts to penalize pixel technology. This Court, by contrast, has repeatedly and emphatically refused to distort statutory text to punish commonplace uses of modern technology. It should follow that same course again here.

A. Plaintiffs Are Seeking To Impose Massive Liability On Distributors And Users Of Pixel Technology

Plaintiffs across the country have launched a torrent of litigation targeting modern analytics technology. They have brought dozens of suits against the companies, like Meta, who provide pixel technology and similar analytics tools.[2] Even more cases—like this one—take aim at developers who rely on these technologies to enhance their websites and serve their users.[3] The motivation for these lawsuits is not hard to spot: Many of the statutes invoked by

---

[2] *See, e.g.*, *Griffith v. TikTok, Inc.*, 697 F. Supp. 3d 963 (C.D. Cal. 2023) (suit against pixel provider TikTok based on pixel usage by various websites, including Etsy and Build-A-Bear); *Popa v. Harriet Carter Gifts, Inc.*, 52 F.4th 121 (3d Cir. 2022) (suit against pixel provider NaviStone based on pixel usage by website selling specialty stairs for pets); *Timothee v. Meta Platforms,* 2026 WL 1130363 (N.D. Cal. Apr. 27, 2026) (suit against pixel provider Meta based on pixel usage by nonprofit food banks).

[3] *See, e.g.*, *Pileggi v. Wash. Newspaper Publ'g Co., LLC*, 146 F.4th 1219 (D.C. Cir. 2025) (suit against *Washington Examiner* news website), *petition for cert. filed* (U.S. Feb. 27, 2026) (No. 25-1040); *Moody v. C2 Educ. Sys., Inc.*, 742 F. Supp. 3d 1072 (C.D. Cal. 2024) (suit against online K-12 tutoring website); *Markels v. AARP*, 689 F. Supp. 3d 722 (N.D. Cal. 2023) (suit against nonprofit AARP website).

plaintiffs potentially expose defendants to thousands of dollars in damages for each violation. By targeting commonplace online activity involving countless transactions every day, plaintiffs can rack up damages demands on a massive scale. But these ambitious attempts to extract millions—or even billions—of dollars in civil penalties require plaintiffs to rewrite the text of these statutes.

The VPPA prohibits "video tape service provider[s]" from disclosing "personally identifiable information" about their customers' video tape rental histories—on pain of $2,500 in statutory damages per violation. 18 U.S.C. § 2710(b)(1), (c)(2)(A). Despite that Blockbuster-era prohibition's poor fit for regulating modern web traffic analytics, plaintiffs have sued dozens of developers using analytics tools like pixel technology under the VPPA.[4] *See* Resp. Br. 9-10. But the VPPA is just one of the many inapposite statutes invoked in recent attacks on modern analytics tools.

Beyond the VPPA, plaintiffs frequently assert that certain uses of these technologies violate federal and state criminal prohibitions on wiretapping, eavesdropping, and surreptitious recording, which likewise carry significant per-violation civil

---

[4] *See, e.g.*, *Cole v. LinkedIn Corp.*, 807 F. Supp. 3d 959 (N.D. Cal. 2025) (suit alleging that professional networking platform LinkedIn violated VPPA by measuring views of video learning courses); *Collins v. Toledo Blade*, 720 F. Supp. 3d 543 (N.D. Ohio 2024) (suit alleging that local newspapers *Toledo Blade* and *Pittsburgh Post-Gazette* violated VPPA by measuring views of video reports); *Osheske v. Silver Cinemas Acquisition Co.*, 700 F. Supp. 3d 921 (C.D. Cal. 2023) (suit alleging that movie theater violated VPPA by measuring online ticket sales).

penalties.[5] And some plaintiffs have even relied on anti-hacking laws like the federal Computer Fraud and Abuse Act (CFAA) or the California Comprehensive Data Access and Fraud Act (CDAFA).[6] Far too many courts have allowed these kinds of claims to proceed, even though they rest on atextual readings of the relevant statutes.

Take wiretapping statutes. Originally enacted in 1968, the federal Wiretap Act prohibits the use of a "device" to "intercept" wire, electronic, or oral communications. *See* 18 U.S.C. §§ 2510(4), 2511(1), (4)(a). This decades-old legislation focused on "objectionable devices" used for those illicit purposes, such as "the martini olive transmitter, the spike mike, the infinity transmitter, and the microphone disguised as a wristwatch, picture frame, cuff link, tie clip, fountain pen, stapler, or cigarette pack." S. Rep.

---

[5] *Casillas v. Six Flags Ent. Corp.*, 812 F. Supp. 3d 1016 (C.D. Cal. 2025) (suit alleging that Six Flags theme park engaged in wiretapping by measuring user activity on its websites); *Heerde v. Learfield Commc'ns, LLC*, 741 F. Supp. 3d 849 (C.D. Cal. 2024) (similar suit against University of Southern California); *Mikulsky v. Bloomingdale's, LLC*, 713 F. Supp. 3d 833 (S.D. Cal. 2024) (similar suit against Bloomingdale's department store).

[6] *See, e.g.*, *Shah v. Cap. One Fin. Corp.*, 768 F. Supp. 3d 1033 (N.D. Cal. 2025) (suit alleging that pixel technology usage by Capital One bank constituted computer hacking under the CFAA, CDAFA, and Stored Communications Act); *Doe I v. Google LLC*, 741 F. Supp. 3d 828 (N.D. Cal. 2024) (suit alleging that Google's pixel technology was a "contaminant"—i.e., a computer virus—that tampered with data under CDAFA); *In re BPS Direct, LLC*, 705 F. Supp. 3d 333 (E.D. Pa. 2023) (suit alleging that BPS Direct and Cabela's retail websites violated CFAA by measuring user activity), *aff'd in part and rev'd in part on other grounds*, 175 F.4th 423 (3d Cir. 2026).

No. 90-1097, at 95 (1968). And in updating the legislation two decades later, Congress took aim at analogous "[e]lectronic hardware making it possible for overzealous law enforcement agencies, industrial spies, and private parties" to intercept private communications. S. Rep. No. 99-541, at 3 (1986). Congress imposed severe punishments on violators, including criminal sanctions and civil penalties. *See* 18 U.S.C. §§ 2520(c)(2)(B), 2511(4)(a).

Many states have similar wiretapping statutes. For instance, the California Invasion of Privacy Act (CIPA)—originally enacted in 1967—criminalizes "attempt[ing] to read, or to learn the contents or meaning of any message" while it is "in transit," Cal. Penal Code § 631(a), as well as "us[ing] an electronic amplifying or recording device" to "eavesdrop upon or record" a "confidential communication," *id.* § 632(a). *See, e.g.*, 18 Pa. Cons. Stat. § 5703; Md. Code Ann., Cts. & Jud. Proc. § 10-402; Mass. Gen. Laws ch. 272, § 99; Fla. Stat. §§ 934.03, 934.10. Like their federal counterpart, these state prohibitions come with stiff criminal and civil penalties commensurate with the legislative goal of combatting "industrial espionage" and "theft of trade secrets." Digest of A.B. 860, at 1 (June 8, 1967). CIPA, for example, imposes on violators up to a year of jail time and civil penalties of "[f]ive thousand dollars ($5,000) per violation." Cal. Penal Code § 637.2; *see id.* §§ 631(a), 632(a).

The text of these criminal prohibitions on wiretapping plainly does not outlaw the distribution or use of pixel technology and other analytics tools. Pixel code—which developers use to understand *their own interactions* with users—is not a wiretapping "device" designed or used to "intercept" the "confidential communications" of other people. And

certainly Meta—which provides pixel code to developers, who then decide how to configure it—does not *itself* "use" the pixel code to "record" or "eavesdrop." *Id.* § 632. Nor does Meta "read" a communication while "in transit," *id.* § 631(a), since Meta merely receives event data *about* a user's actions on a website. Simply put, Meta's distribution and developers' use of code designed to improve website functionality and enable targeted advertising looks nothing like the highly invasive conduct that wiretapping statutes proscribe.

None of this has stopped plaintiffs from claiming that every time pixel code transmits data about web activity across millions of users every day, developers using pixel technology and companies distributing it violate the criminal wiretapping laws, purportedly to the tune of many millions (or billions) of dollars in civil penalties. Some courts have correctly rejected such claims, recognizing that "data analytics for web traffic is worlds different from wiretapping," and thus not subject to criminal sanctions and civil penalties. *Doe v. Eating Recovery Ctr. LLC*, 806 F. Supp. 3d 1109, 1119 (N.D. Cal. 2025) (Chhabria, J.); *see also Moss v. ResortPass Inc.*, 2025 WL 3452360, at *2 (Cal. Super. Ct. Oct. 30, 2025). But many others have let wiretapping claims proceed, against developers and pixel providers alike. *See, e.g.*, *Heerde*, 741 F. Supp. 3d at 858-65; *In re Meta Pixel Healthcare Litig.*, 647 F. Supp. 3d 778, 798-99 (N.D. Cal. 2022); *Smith v. Google, LLC*, 735 F. Supp. 3d 1188, 1199-1202 (N.D. Cal. 2024); *Griffith v. TikTok, Inc.*, 697 F. Supp. 3d 963, 973 (C.D. Cal. 2023); *Casillas*, 812 F. Supp. 3d at 1029-31.

Claims that pixel technology violates anti-hacking statutes are equally misguided. Congress enacted the

federal Computer Fraud and Abuse Act (CFAA) to punish "hackers" who "coopt computers for illegal ends," like theft and fraud. *Van Buren v. United States*, 593 U.S. 374, 378-79 (2021); *see* 18 U.S.C. § 1030 (prohibiting, *inter alia*, unauthorized access to national defense information, credit files, and government computers). Many states, such as California, have enacted similar computer-crime laws to prevent similar conduct like "tampering, interference, damage, and unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a).

Pixel code does none of those things. When a website that incorporates pixel code analyzes website interactions, it *generates* event data based on user activity—and does not tamper with, interfere with, or damage a user's own preexisting data (like personal emails, documents, photographs, and so on). *See Doe v. Tenet Healthcare Corp.*, 789 F. Supp. 3d 814, 826-27, 844-45 (E.D. Cal. 2025); *Heiting v. Taro Pharms. USA, Inc.*, 709 F. Supp. 3d 1007, 1021 (C.D. Cal. 2023).

Pixel code's event generation and analytics functions thus look nothing like the "'computer crime' and hacking" that CDAFA (and the CFAA) were "enacted to combat." *Heiting*, 709 F. Supp. 3d at 1020. Despite that obvious mismatch, plaintiffs have persisted in bringing claims under both statutes, and some courts have stretched CDAFA's text to cover use of pixel technology. *See, e.g.*, *In re Meta Pixel Healthcare Litig.*, 713 F. Supp. 3d 650, 655-57 (N.D. Cal. 2024); *Brown v. Google LLC*, 685 F. Supp. 3d 909, 939-40 (N.D. Cal. 2023); *Zarif v. Hwareh.com, Inc.*, 789 F. Supp. 3d 880, 899-900 (S.D. Cal. 2025); *Smith*

v. Rack Room Shoes, Inc., 2025 WL 1085169, at *6 (N.D. Cal. Apr. 4, 2025).[7]

These are just some examples of plaintiffs and courts invoking ill-suited statutes to regulate pixel technology. Websites that undertake the online equivalent of shopkeepers observing customer habits in their own brick-and-mortar stores are not wiretapping, eavesdropping upon, or hacking their users. Yet numerous erroneous decisions have held otherwise. As Judge Chhabria has observed, this "state of affairs" is "untenable." *Eating Recovery Ctr.*, 806 F. Supp. 3d at 1112. "Courts are issuing conflicting rulings, and companies have no way of telling whether their online business activities will subject them to liability." *Id.*

Left unchecked, this trend risks imposing crushing liability—even criminal sanctions—on providers and users of pixel technology that will stifle innovation and competition across the internet. Many developers may choose to forego using pixel technology rather than risk jail time or massive civil liability, undermining their website's effectiveness and erasing the benefits of personalized advertising. That outcome suits no one.

B. This Court Should Adhere To The VPPA's Text

This Court should stem the tide of lawsuits seeking to punish the distribution and use of pixel technology and similar analytics tools under inapposite statutes. The Court has repeatedly

---

[7] Unlike CDAFA, the CFAA generally requires plaintiffs to allege $5,000 in damage or loss over a one-year period, which somewhat limits CFAA claims based on analytics technology. *See* 18 U.S.C. § 1030(c)(4)(A)(i).

rejected attempts to read narrow statutory text to sweep in commonplace uses of modern technology. It should do so again here and reject Salazar's boundless construction of the VPPA. Doing so will steer other courts away from similarly distorting other statutes.

1. This Court Has Repeatedly Refused To Read Statutes To Penalize Routine Uses Of Modern Technology

In several cases, this Court has been asked to stretch statutory text in service of punishing people and businesses for using modern technology in routine ways. And each time, this Court said no.

In *Facebook, Inc. v. Duguid*, the Court confronted another statute imposing statutory damages—the Telephone Consumer Protection Act (TCPA)—that the plaintiffs' bar had deployed to launch a sweeping litigation campaign based on expansive liability theories. 592 U.S. 395, 398-99 (2021). Congress enacted the TCPA in 1991 to combat robocalls. *Id.* at 399. Congress was concerned about so-called "autodialer technology"—i.e., systems that could automatically dial random or sequential blocks of phone numbers—because that technology could, at the time, "'seiz[e] the telephone lines of public emergency services'" and "simultaneously tie up all the lines of any business with sequentially numbered phone lines." *Id.* at 399-400 (quoting H.R. Rep. No. 102-317, at 24 (1991)). As a result, the TCPA prohibited making certain calls using an "automatic telephone dialing system" with the capacity "to store or produce telephone numbers to be called, using a random or sequential number generator." 47 U.S.C. § 227(a)(1). Congress also created a private right of

action permitting recovery up to $1,500 per violation. *Id.* § 227(b)(3).

Two decades later, the plaintiffs' bar dusted off the TCPA to seek massive damages against numerous companies (including Meta) for a completely different technology: electronic features that could send automated text messages. Even though text messages did not exist when the TCPA was enacted in 1991, a flood of lawsuits alleged that features used to send such alerts were illegal "automatic telephone dialing system[s]." *Duguid*, 592 U.S. at 400 (citation omitted).[8]

In *Duguid*, the plaintiffs alleged that Meta (then known as Facebook) violated the TCPA by offering a two-step authentication security feature, which would automatically "send[] users 'login notification' text messages when an attempt [wa]s made to access their Facebook account from an unknown device or browser." *Id.* The Ninth Circuit agreed that this login notification feature was an unlawful automatic telephone dialing system, even though the TCPA defined the term as systems "using a random or sequential number generator." *Id.* at 402 (quoting 47 U.S.C. § 227(a)(1)).

---

[8] *See, e.g.*, *Gadelhak v. AT&T Servs., Inc.*, 950 F.3d 458, 460 (7th Cir. 2020) (Barrett, J.) (suit asserting TCPA liability for five text messages surveying customer service satisfaction), *cert. denied*, 141 S. Ct. 2552 (2021); *Marks v. Crunch San Diego, LLC*, 904 F.3d 1041, 1048 (9th Cir. 2018) (suit asserting TCPA liability for three text messages from fitness gym to current member); *Sherman v. Yahoo! Inc.*, 997 F. Supp. 2d 1129, 1136 (S.D. Cal. 2014) (suit asserting TCPA liability for one text message notifying recipient that he had received an instant message on the Yahoo! Messenger service).

This Court unanimously rejected that attempt to reshape the TCPA. Starting with the text, the Court construed "automatic telephone dialing system" to include only technology that met all elements of its statutory definition—including "a random or sequential number generator," something Facebook's login notification feature lacked. *Id.* at 400-04. The "statutory context" confirmed that narrow reading focused on autodialers: Congress had "target[ed] a unique type of telemarketing equipment" because it "risk[ed] dialing emergency lines randomly or tying up all the sequentially numbered lines at a single entity." *Id.* at 405. As the Court explained, the plaintiff's expansive reading "would take a chainsaw to these nuanced problems when Congress meant to use a scalpel." *Id.*

The Court also recognized that adopting the plaintiffs' more expansive reading would shut down post-1991 technological innovations that the TCPA was never meant to punish. It noted that the plaintiffs' theory would "classify[] almost all modern cell phones as autodialers" and thus "affect ordinary cell phone owners in the course of commonplace usage, such as speed dialing or sending automated text message responses." *Id.* at 406-07. The Court refused to countenance such a radical reimagination of the TCPA. *See id.*

This Court took a similar course in *Van Buren*, where the government pressed an expansive interpretation of the CFAA. In *Van Buren*, a police sergeant with access to a law enforcement database had allegedly misused that access to conduct improper license-plate searches. 593 U.S. at 378. The government charged him under a CFAA provision making it illegal "to access a computer with

authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(a)(2), (e)(6). The Eleventh Circuit upheld the conviction, reasoning that this provision should be read broadly to encompass anyone who "misuse[s] access" to a computer system or data "that they otherwise have." *Van Buren*, 593 U.S. at 381 (citation omitted). It thus concluded that the police sergeant "had violated the CFAA by accessing the law enforcement database for an 'inappropriate reason.'" *Id.* (citation omitted).

As in *Duguid*, this Court reversed. The Court explained that the CFAA's prohibition on obtaining information from a computer that the user "'is not entitled to so obtain'" is "best read to refer" only to information that the person lacks authorization to access at all. *Id.* at 384. A "wider look at the statute's structure" reinforced that interpretation. *Id.* at 389 (citation omitted). The CFAA's "focus [is] on technological harms"—"such as the corruption of files"—that are "'the typical consequences of hacking,'" not "'misuse' of sensitive information that employees may permissibly access." *Id.* at 391-92 (citation omitted).

"To top it all off," the Court emphasized, "the Government's interpretation of the statute would attach criminal penalties to a breathtaking amount of commonplace computer activity." *Id.* at 393-94. Interpreting the CFAA broadly would potentially subject "an employee who sends a personal e-mail or reads the news using her work computer" to prosecution, and "criminalize everything from embellishing an online-dating profile to using a pseudonym on Facebook." *Id.* at 394. This Court found it highly unlikely that Congress intended to

make "millions of otherwise law-abiding citizens . . . criminals," which "underscore[d] the implausibility" of the Government's view. *Id.* Text, context, and common sense thus all aligned to cabin the CFAA's reach.

The Court adhered to these same principles in *Cox Communications, Inc. v. Sony Music Entertainment*, 146 S. Ct. 959 (2026), by limiting liability for companies that merely distribute technology capable of misuse by others. More specifically, in *Cox* this Court refused to hold an internet service provider "liable merely for failing to terminate Internet service to infringing accounts," which would vastly "expand secondary copyright liability." *Id.* at 968. The Court was "loath to expand" secondary liability under the Copyright Act beyond the scope established in prior precedents, particularly since the statute lacks any provision "expressly render[ing] anyone liable for infringement committed by another." *Id.* at 967 (quoting *Sony Corp. of Am. v. Universal City Studios, Inc.*, 464 U.S. 417, 434 (1984)). And because "[c]ountless people use the internet for legal activities," the Court declined to risk stifling lawful internet activity by exposing internet service providers to sweeping civil liability for third party users' alleged unlawful activities. *Id.* at 964.

Cox reaffirmed that "'mere indifferent supposition or knowledge on the part of [a] seller' that the buyer will use the product unlawfully" is not enough to impose liability on the seller for the buyer's misuse. *Id.* at 968 (citation omitted); *see* Restatement (Third) of Torts: Physical & Emotional Harm § 1, cmt. e (2010). This established rule ensures that the general public will remain "free[] to engage" in the lawful use of widely available technologies, even though bad

actors could misuse them. *Sony*, 464 U.S. at 442; *accord Twitter, Inc. v. Taamneh*, 598 U.S. 471, 502-03 (2023) (declining to impose liability on platforms used by "billions of people" for "interactions that once took place via mail, on the phone, or in public areas" despite misconduct by "some bad actors"). Because the *Cox* defendant "simply provided Internet access, which is used for many purposes other than copyright infringement," the Court rejected liability. 146 S. Ct. at 968.

Together, *Duguid*, *Van Buren*, and *Cox* teach that courts must adhere to textual limits on liability, rather than stretch statutes for the sake of penalizing commonplace uses and distribution of modern technology.

2. The Court Should Take The Same Approach With The VPPA

Once again, this Court is being asked to stretch a carefully circumscribed statute to reach routine use of an everyday technology that was never contemplated when Congress chose its words. And once again, this Court should decline. Consistent with *Duguid*, *Van Buren*, and *Cox*, the Court should hew to the VPPA's text and reject Salazar's boundless reading.

The VPPA's text establishes clear guardrails on liability. The VPPA applies only to "video tape service provider[s]," which the statute defines as someone transacting in "video cassette tapes or similar audiovisual materials." 18 U.S.C. § 2710(a)(4). This "definition excludes" anyone who "does not [transact in] such technology." *Duguid*, 592 U.S. at 404. In addition, the VPPA generally prohibits those providers from knowingly disclosing the "personally identifiable information" of "any consumer of such

provider[s]." 18 U.S.C. § 2710(b)(1). In this context, "personally identifiable information" must actually "identif[y] a person as having requested or obtained specific video materials." *Id.* § 2710(a)(3). And a consumer means any "renter, purchaser, or subscriber of goods or services from a video tape service provider." *Id.* § 2710(a)(1).

The VPPA's text thus precludes Salazar's claims several times over. To begin, Salazar is not a "consumer" of a video tape service provider. *Id.* § 2710(a)(1), (b)(1). He signed up for a free email newsletter, and incidentally may have viewed free video content on 247Sports' website. He thus did not "rent[], purchase[], or subscribe[]" to audiovisual materials, as the statute requires. *See id.* § 2710(a)(1). As Respondent explains, "one becomes a VPPA consumer by renting, purchasing, or subscribing to the audiovisual goods or services that a video provider rents, sells, or delivers," not by purchasing unrelated goods or signing up for unrelated services. Resp. Br. 14.

Furthermore, 247Sports is not a "video tape service provider" because it is not in the business of "rent[ing], s[elling], or deliver[ing] . . . prerecorded video cassette tapes or similar audiovisual materials." 18 U.S.C. § 2710(a)(4). Rather, 247Sports provides "news" about "college sports" in multiple forms, including via free "video clips" on its website. BIO 5. And regardless, 247Sports' use of Meta's Pixel code did not disclose "personally identifiable information" within the meaning of the VPPA—i.e., information that "identifies a person as having requested or obtained specific video materials," 18 U.S.C. § 2710(a)(3)—because "an ordinary person" could not readily "identify a consumer's video-watching habits"

by looking at raw pixel event data, which is "interspersed with many characters, numbers, and letters," *Solomon v. Flipps Media, Inc.*, 136 F.4th 41, 52, 54 (2d Cir.), *cert. denied*, 146 S. Ct. 885 (2025); *accord In re Nickelodeon Consumer Priv. Litig.*, 827 F.3d 262, 278 (3d Cir. 2016), *cert. denied*, 580 U.S. 1048 (2017). Thus, from top to bottom, the VPPA's text confirms that the statute does not reach 247Sports' routine use of Pixel code.

What the statutory text provides, context confirms. Congress enacted the VPPA after Judge Robert Bork's video tape rental history was disclosed during his failed confirmation hearings. S. Rep. No. 100-599, at 5 (1988). Congress accordingly selected a "narrow statutory design" focused on protecting the privacy of video tape rental histories and analogous transactions. *Duguid*, 592 U.S. at 408. It did not, as Salazar insists, draft a statute reaching *anyone* who posts videos on their website, offers sales or subscriptions, and also happens to use modern analytics tools. *See* Resp. Br. 47-49. This Court should respect the careful limits on liability that Congress established, just as it has done many times before.

* * *

Limiting the VPPA's reach in this case would set a valuable example for other courts faced with lawsuits challenging the distribution and use of modern analytics tools like pixel technology. It would reaffirm that statutory text must be followed faithfully, not contorted to prohibit ubiquitous and beneficial new technologies. And it would send a much-needed signal that pixel technology does not violate prohibitions on wiretapping, eavesdropping, and

hacking. This Court should reject Salazar's claims, and in so doing leave room for the innovations that today's online ecosystem needs to thrive.

CONCLUSION

This Court should affirm the Sixth Circuit's judgment.

Respectfully submitted,

MELANIE BLUNSCHI
NICHOLAS ROSELLINI
LATHAM & WATKINS LLP
505 Montgomery Street
Suite 2000
San Francisco, CA 94111

NIKKI STITT SOKOL
CARRIE J. BODNER
META PLATFORMS, INC.
1 Hacker Way
Menlo Park, CA 94025

ROMAN MARTINEZ
Counsel of Record
ANDREW B. CLUBOK
SUSAN E. ENGEL
SOREN J. SCHMIDT
RUTH HIRSCH
LATHAM & WATKINS LLP
555 Eleventh Street, NW
Suite 1000
Washington, DC 20004
(202) 637-3377
roman.martinez@lw.com

Counsel for Amicus Curiae *Meta Platforms, Inc.*

June 30, 2026